(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－142398
（P2001－142398A）
(43)公開日　平成13年５月25日(2001.5.25)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｚ	
			６４０Ｂ	

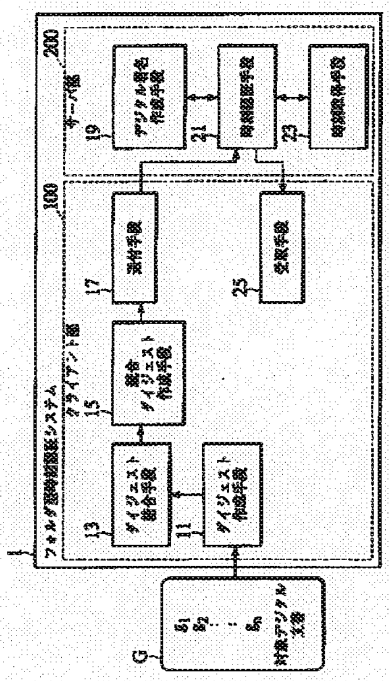
審査請求　未請求　請求項の数37　ＯＬ　（全 20 頁）

(21)出願番号　特願2000－266194(P2000－266194)
(22)出願日　平成12年９月１日(2000.9.1)
(31)優先権主張番号　特願平11－247993
(32)優先日　平成11年９月１日(1999.9.1)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平11－247994
(32)優先日　平成11年９月１日(1999.9.1)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　田倉　昭
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　小野　論
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100083806
弁理士　三好　秀和　（外１名）

(54)【発明の名称】　フォルダ型時刻認証システムおよび分散時刻認証システム

(57)【要約】
【課題】　パソコン上のデジタル文書を日常的に履歴の残る記録とし、かつ変更作成記録を第三者に証明することが可能となる時刻認証システムを提供すること。
【解決手段】　時刻認証システムにおいて、クライアント装置は、複数のデジタル文書に対する複数のダイジェストを作成し、作成された複数のダイジェストを結合し、結合された複数のダイジェストから統合ダイジェストを作成し、作成された統合ダイジェストを含んだ時刻認証要求をサーバ装置に送付して、サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取る。サーバ装置は、時刻認証要求に応じて取得された時刻情報と統合ダイジェストを結合して求められた時刻印付きデジタル文書と、時刻印付きデジタル文書に対するデジタル署名とを含んだ時刻認証証明書を作成する。



1

【特許請求の範囲】

【請求項１】　クライアント装置とサーバ装置からなる時刻認証システムであって、クライアント装置は、
複数のデジタル文書に対する複数のダイジェストを作成するダイジェスト作成手段と、
このダイジェスト作成手段により作成された複数のダイジェストを結合するダイジェスト結合手段と、
このダイジェスト結合手段により結合された複数のダイジェストから統合ダイジェストを作成する統合ダイジェスト作成手段と、
この統合ダイジェスト作成手段により作成された統合ダイジェストを含んだ時刻認証要求をサーバ装置に送付する送付手段と、
サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取る受取手段とを有し、
サーバ装置は、時刻認証要求に応じて取得された時刻情報と統合ダイジェストを結合して求められた時刻印付きデジタル文書と、時刻印付きデジタル文書に対するデジタル署名とを含んだ時刻認証証明書を作成することを特徴とする時刻認証システム。

【請求項２】　クライアント装置は更に、パソコンまたはネットワーク上のデジタル文書から前記複数のデジタル文書を、ファイルまたはフォルダ単位で指定するデジタル文書指定手段を有することを特徴とする請求項１記載の時刻認証システム。

【請求項３】　デジタル文書指定手段は、前記複数のデジタル文書に以前に取得した時刻認証証明書が含まれるように、前記複数のデジタル文書を指定することを特徴とする請求項２記載の時刻認証システム。

【請求項４】　クライアント装置は更に、ダイジェスト作成手段に定期的なダイジェスト作成時刻を指定して、ダイジェスト作成手段がこの定期的なダイジェスト作成時刻に前記複数のダイジェストを定期的に作成するようにする時刻指定手段を有することを特徴とする請求項１記載の時刻認証システム。

【請求項５】　クライアント装置は更に、受取手段で受け取った時刻認証証明書に含まれるデジタル署名が正しいか否か検証する検証手段を有することを特徴とする請求項１記載の時刻認証システム。

【請求項６】　クライアント装置は更に、受取手段で受け取った時刻認証証明書に含まれる時刻印付きデジタル文書によって示される時刻が、送付手段における時刻認証要求の送付時刻と、受取手段における時刻認証証明書の受取時刻の間にあることを検証する検証手段を有することを特徴とする請求項１記載の時刻認証システム。

【請求項７】　サーバ装置は、
統合ダイジェストと時刻情報を結合して時刻印付きデジタル文書を求め、時刻印付きデジタル文書に対するデジタル署名を生成するデジタル署名手段と、
このデジタル署名手段により生成された時刻印付きデジタル文書とデジタル署名から時刻認証証明書を作成する時刻認証証明書作成手段と、
を有することを特徴とする請求項１記載の時刻認証システム。

2

【請求項８】　サーバ装置は、
複数の時刻取得手段で、各時刻取得手段は、時刻認証要求に応じて、他の時刻取得手段とは独立に、所定の一定の刻み幅で与えられた前記時刻情報を順次取得する時刻取得手段と、
これら複数の時刻取得手段に対応して設けられた複数の結合手段で、各結合手段は、他の結合手段とは独立に、対応する時刻取得手段により順次取得された時刻情報を統合ダイジェストを含んだデータを順次結合して複数の時刻印付きデジタル文書を作成する結合手段と、
これら複数の結合手段に対応して設けられた複数のデジタル署名手段で、各デジタル署名手段は、他のデジタル署名手段とは独立に、対応する結合手段により作成された各時刻印付きデジタル文書に対するデジタル署名を生成するデジタル署名手段と、
複数のデジタル署名手段によって生成された複数のデジタル署名から、複数のデジタル署名手段によって同一時刻の時刻印付きデジタル文書に対して生成された複数のデジタル署名を、各デジタル署名手段毎に一つずつ選択し、選択されたデジタル署名から統合デジタル署名を作成する統合デジタル署名作成手段と、
この統合デジタル署名作成手段により作成された統合デジタル署名と前記同一時刻の時刻印付きデジタル文書から時刻認証証明書を作成する時刻認証証明書作成手段と、
を有することを特徴とする請求項１記載の時刻認証システム。

【請求項９】　各デジタル署名手段は、前記同一時刻になる可能性のない時刻の時刻印付きデジタル文書の少なくとも一つに対するデジタル署名を生成しないように制御されることを特徴とする請求項８記載の時刻認証システム。

【請求項１０】　統合デジタル署名作成手段と時刻認証証明書作成手段が時刻認証機関を構成し、時刻取得手段と結合手段とデジタル署名手段の各組が分散部分時刻認証機関を構成することを特徴とする請求項８記載の時刻認証システム。

【請求項１１】　複数のデジタル文書に対する複数のダイジェストを作成するダイジェスト作成手段と、
このダイジェスト作成手段により作成された複数のダイジェストを結合するダイジェスト結合手段と、
このダイジェスト結合手段により結合された複数のダイジェストから統合ダイジェストを作成する統合ダイジェスト作成手段と、
この統合ダイジェスト作成手段により作成された統合ダイジェストを含んだ時刻認証要求を時刻認証システムの

サーバ装置に送付する送付手段と、
サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取る受取手段と、
を有することを特徴とする時刻認証システムのクライアント装置。

【請求項１２】　パソコンまたはネットワーク上のデジタル文書から前記複数のデジタル文書を、ファイルまたはフォルダ単位で指定するデジタル文書指定手段を更に有することを特徴とする請求項１１記載のクライアント装置。

【請求項１３】　デジタル文書指定手段は、前記複数のデジタル文書に以前に取得した時刻認証証明書が含まれるように、前記複数のデジタル文書を指定することを特徴とする請求項１２記載のクライアント装置。

【請求項１４】　ダイジェスト作成手段に定期的なダイジェスト作成時刻を指定して、ダイジェスト作成手段がこの定期的なダイジェスト作成時刻に前記複数のダイジェストを定期的に作成するようにする時刻指定手段を更に有することを特徴とする請求項１１記載のクライアント装置。

【請求項１５】　受取手段で受け取った時刻認証証明書に含まれるデジタル署名が正しいか否か検証する検証手段を更に有することを特徴とする請求項１１記載のクライアント装置。

【請求項１６】　受取手段で受け取った時刻認証証明書に含まれる時刻印付きデジタル文書によって示される時刻が、送付手段における時刻認証要求の送付時刻と、受取手段における時刻認証証明書の受取時刻の間にあることを検証する検証手段を更に有することを特徴とする請求項１１記載のクライアント装置。

【請求項１７】　複数の時刻取得手段で、各時刻取得手段は、時刻認証要求に応じて、他の時刻取得手段とは独立に、所定の一定の刻み幅で与えられた前記時刻情報を順次取得する時刻取得手段と、
これら複数の時刻取得手段に対応して設けられた複数の結合手段で、各結合手段は、他の結合手段とは独立に、対応する時刻取得手段により順次取得された時刻情報を統合ダイジェストを含んだデータを順次結合して複数の時刻印付きデジタル文書を作成する結合手段と、
これら複数の結合手段に対応して設けられた複数のデジタル署名手段で、各デジタル署名手段は、他のデジタル署名手段とは独立に、対応する結合手段により作成された各時刻印付きデジタル文書に対するデジタル署名を生成するデジタル署名手段と、
複数のデジタル署名手段によって生成された複数のデジタル署名から、複数のデジタル署名手段によって同一時刻の時刻印付きデジタル文書に対して生成された複数のデジタル署名を、各デジタル署名手段毎に一つずつ選択し、選択されたデジタル署名から統合デジタル署名を作成する統合デジタル署名作成手段と、

この統合デジタル署名作成手段により作成された統合デジタル署名と前記同一時刻の時刻印付きデジタル文書から時刻認証証明書を作成する時刻認証証明書作成手段と、
を有することを特徴とする時刻認証システムのサーバ装置。

【請求項１８】　各デジタル署名手段は、前記同一時刻になる可能性のない時刻の時刻印付きデジタル文書の少なくとも一つに対するデジタル署名を生成しないように制御されることを特徴とする請求項１７記載のサーバ装置。

【請求項１９】　統合デジタル署名作成手段と時刻認証証明書作成手段が時刻認証機関を構成し、時刻取得手段と結合手段とデジタル署名手段の各組が分散部分時刻認証機関を構成することを特徴とする請求項１７記載のサーバ装置。

【請求項２０】　クライアント装置とサーバ装置からなる時刻認証システムにおける時刻認証方法であって、
（ａ）クライアント装置において、複数のデジタル文書に対する複数のダイジェストを作成するステップと、
（ｂ）クライアント装置において、ステップ（ａ）により作成された複数のダイジェストを結合するステップと、
（ｃ）クライアント装置のおいて、ステップ（ｂ）により結合された複数のダイジェストから統合ダイジェストを作成するステップと、
（ｄ）ステップ（ｃ）により作成された統合ダイジェストを含んだ時刻認証要求をクライアント装置からサーバ装置に送付するステップと、
（ｅ）サーバ装置において、時刻認証要求に応じて取得された時刻情報と統合ダイジェストを結合して求められた時刻印付きデジタル文書と、時刻印付きデジタル文書に対するデジタル署名とを含んだ時刻認証証明書を作成するステップと、
（ｆ）クライアント装置において、サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取るステップと、
を有することを特徴とする時刻認証方法。

【請求項２１】　クライアント装置において、パソコンまたはネットワーク上のデジタル文書から前記複数のデジタル文書を、ファイルまたはフォルダ単位で指定するステップを更に有することを特徴とする請求項２０記載の時刻認証方法。

【請求項２２】　前記指定するステップは、前記複数のデジタル文書に以前に取得した時刻認証証明書が含まれるように、前記複数のデジタル文書を指定することを特徴とする請求項２１記載の時刻認証方法。

【請求項２３】　クライアント装置において、定期的なダイジェスト作成時刻を指定して、ステップ（ａ）がこの定期的なダイジェスト作成時刻に前記複数のダイジェ

ストを定期的に作成するようにするステップを更に有することを特徴とする請求項２０記載の時刻認証方法。

【請求項２４】　クライアント装置において、ステップ（ｆ）で受け取った時刻認証証明書に含まれるデジタル署名が正しいか否か検証するステップを更に有することを特徴とする請求項２０記載の時刻認証方法。

【請求項２５】　クライアント装置において、ステップ（ｆ）で受け取った時刻認証証明書に含まれる時刻印付きデジタル文書によって示される時刻が、ステップ（ｄ）における時刻認証要求の送付時刻と、ステップ（ｆ）における時刻認証証明書の受取時刻の間にあることを検証するステップを更に有することを特徴とする請求項２０記載の時刻認証方法。

【請求項２６】　前記ステップ（ｅ）は、

（ｅ１）サーバ装置の複数の時刻取得手段の各時刻取得手段において、時刻認証要求に応じて、他の時刻取得手段とは独立に、所定の一定の刻み幅で与えられた前記時刻情報を順次取得するステップと、

（ｅ２）サーバ装置のこれら複数の時刻取得手段に対応して設けられた複数の結合手段の各結合手段において、他の結合手段とは独立に、対応する時刻取得手段により順次取得された時刻情報を統合ダイジェストを含んだデータを順次結合して複数の時刻印付きデジタル文書を作成するステップと、

（ｅ３）サーバ装置のこれら複数の結合手段に対応して設けられた複数のデジタル署名手段の各デジタル署名手段において、他のデジタル署名手段とは独立に、対応する結合手段により作成された各時刻印付きデジタル文書に対するデジタル署名を生成するステップと、

（ｅ４）複数のデジタル署名手段によって生成された複数のデジタル署名から、複数のデジタル署名手段によって同一時刻の時刻印付きデジタル文書に対して生成された複数のデジタル署名を、各デジタル署名手段毎に一つずつ選択し、選択されたデジタル署名から統合デジタル署名を作成するステップと、

（ｅ５）ステップ（ｅ４）により作成された統合デジタル署名と前記同一時刻の時刻印付きデジタル文書から時刻認証証明書を作成するステップと、

を有することを特徴とする請求項２０記載の時刻認証方法。

【請求項２７】　前記ステップ（ｅ３）において、各デジタル署名手段は、前記同一時刻になる可能性のない時刻の時刻印付きデジタル文書の少なくとも一つに対するデジタル署名を生成しないように制御されることを特徴とする請求項２６記載の時刻認証方法。

【請求項２８】　時刻認証システムのクライアント装置において時刻認証サービスを受ける方法であって、

（ａ）複数のデジタル文書に対する複数のダイジェストを作成するステップと、

（ｂ）ステップ（ａ）により作成された複数のダイジェストを結合するステップと、

（ｃ）ステップ（ｂ）により結合された複数のダイジェストから統合ダイジェストを作成するステップと、

（ｄ）ステップ（ｃ）により作成された統合ダイジェストを含んだ時刻認証要求を時刻認証システムのサーバ装置に送付するステップと、

（ｅ）サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取るステップと、

を有することを特徴とする時刻認証サービスを受ける方法。

【請求項２９】　パソコンまたはネットワーク上のデジタル文書から前記複数のデジタル文書を、ファイルまたはフォルダ単位で指定するステップを更に有することを特徴とする請求項２８記載の時刻認証サービスを受ける方法。

【請求項３０】　前記指定するステップは、前記複数のデジタル文書に以前に取得した時刻認証証明書が含まれるように、前記複数のデジタル文書を指定することを特徴とする請求項２９記載の時刻認証サービスを受ける方法。

【請求項３１】　クライアント装置において、定期的なダイジェスト作成時刻を指定して、ステップ（ａ）がこの定期的なダイジェスト作成時刻に前記複数のダイジェストを定期的に作成するようにするステップを更に有することを特徴とする請求項２８記載の時刻認証サービスを受ける方法。

【請求項３２】　時刻認証証明書は、時刻認証要求に応じて取得された時刻情報と統合ダイジェストを結合して求められた時刻印付きデジタル文書と、時刻印付きデジタル文書に対するデジタル署名とを含んでおり、

クライアント装置において、ステップ（ｅ）で受け取った時刻認証証明書に含まれるデジタル署名が正しいか否か検証するステップを更に有することを特徴とする請求項２８記載の時刻認証サービスを受ける方法。

【請求項３３】　時刻認証証明書は、時刻認証要求に応じて取得された時刻情報と統合ダイジェストを結合して求められた時刻印付きデジタル文書と、時刻印付きデジタル文書に対するデジタル署名とを含んでおり、

クライアント装置において、ステップ（ｅ）で受け取った時刻認証証明書に含まれる時刻印付きデジタル文書によって示される時刻が、ステップ（ｄ）における時刻認証要求の送付時刻と、ステップ（ｅ）における時刻認証証明書の受取時刻の間にあることを検証するステップを更に有することを特徴とする請求項２８記載の時刻認証サービスを受ける方法。

【請求項３４】　時刻認証システムのサーバ装置において時刻認証サービスを提供する方法であって、

（ａ）サーバ装置の複数の時刻取得手段の各時刻取得手段において、時刻認証要求に応じて、他の時刻取得手段とは独立に、所定の一定の刻み幅で与えられた前記時刻

情報を順次取得するステップと、
（ｂ）サーバ装置のこれら複数の時刻取得手段に対応して設けられた複数の結合手段の各結合手段において、他の結合手段とは独立に、対応する時刻取得手段により順次取得された時刻情報を統合ダイジェストを含んだデータを順次結合して複数の時刻印付きデジタル文書を作成するステップと、
（ｃ）サーバ装置のこれら複数の結合手段に対応して設けられた複数のデジタル署名手段の各デジタル署名手段において、他のデジタル署名手段とは独立に、対応する結合手段により作成された各時刻印付きデジタル文書に対するデジタル署名を生成するステップと、
（ｄ）複数のデジタル署名手段によって生成された複数のデジタル署名から、複数のデジタル署名手段によって同一時刻の時刻印付きデジタル文書に対して生成された複数のデジタル署名を、各デジタル署名手段毎に一つずつ選択し、選択されたデジタル署名から統合デジタル署名を作成するステップと、
（ｅ）ステップ（ｄ）により作成された統合デジタル署名と前記同一時刻の時刻印付きデジタル文書から時刻認証証明書を作成するステップと、
を有することを特徴とする時刻認証サービスを提供する方法。
【請求項３５】　前記ステップ（ｃ）において、各デジタル署名手段は、前記同一時刻になる可能性のない時刻の時刻印付きデジタル文書の少なくとも一つに対するデジタル署名を生成しないように制御されることを特徴とする請求項３４記載の時刻認証サービスを提供する方法。
【請求項３６】　コンピュータを時刻認証システムのクライアント装置として機能させるためのコンピュータ読み取り可能なプログラムコードを格納したコンピュータ利用可能な記録媒体であって、該コンピュータ読み取り可能なプログラムコードは、
複数のデジタル文書に対する複数のダイジェストを作成する第一のプログラムコードと、
この第一のプログラムコードにより作成された複数のダイジェストを結合する第二のプログラムコードと、
この第二のプログラムコードにより結合された複数のダイジェストから統合ダイジェストを作成する第三のプログラムコードと、
この第三のプログラムコードにより作成された統合ダイジェストを含んだ時刻認証要求を時刻認証システムのサーバ装置に送付する第四のプログラムコードと、
サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取る第五のプログラムコードと、
を有することを特徴とする記録媒体。
【請求項３７】　少なくとも一つのコンピュータを時刻認証システムのサーバ装置として機能させるためのコンピュータ読み取り可能なプログラムコードを格納したコンピュータ利用可能な記録媒体であって、該コンピュータ読み取り可能なプログラムコードは、

複数の時刻取得手段で、各時刻取得手段は、時刻認証要求に応じて、他の時刻取得手段とは独立に、所定の一定の刻み幅で与えられた前記時刻情報を順次取得する時刻取得手段を実現するための第一のプログラムコードと、
これら複数の時刻取得手段に対応して設けられた複数の結合手段で、各結合手段は、他の結合手段とは独立に、対応する時刻取得手段により順次取得された時刻情報を統合ダイジェストを含んだデータを順次結合して複数の時刻印付きデジタル文書を作成する結合手段を実現するための第二のプログラムコードと、
これら複数の結合手段に対応して設けられた複数のデジタル署名手段で、各デジタル署名手段は、他のデジタル署名手段とは独立に、対応する結合手段により作成された各時刻印付きデジタル文書に対するデジタル署名を生成するデジタル署名手段を実現するための第三のプログラムコードと、
複数のデジタル署名手段によって生成された複数のデジタル署名から、複数のデジタル署名手段によって同一時刻の時刻印付きデジタル文書に対して生成された複数のデジタル署名を、各デジタル署名手段毎に一つずつ選択し、選択されたデジタル署名から統合デジタル署名を作成す第四のプログラムコードと、
この統合デジタル署名作成手段により作成された統合デジタル署名と前記同一時刻の時刻印付きデジタル文書から時刻認証証明書を作成する第五のプログラムコードと、
を有することを特徴とする記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はデジタル文書に時刻印を押すサービスにおいて、デジタル文書が時刻印を押された時点以降において変更されてなく、かつ確かに時刻印が押された時点で対象とするデジタル文書が存在していたことを証明することを可能とするフォルダ型時刻認証システムおよび分散時刻認証システムに関する。
【０００２】
【従来の技術】例えば米国における先発明主義に基づく特許制度の下では日付の入った研究ノートが優先権を証明する証拠として用いることが可能であり、さらに日付の付けられた家計簿は確定申告における支出記録として使うことができることが知られる。一方、パソコンが日常的に使用されるようになるにつれ、研究ノートや家計簿などの日常記録をパソコンを用いて行うことがごく一般的になってきている。
【０００３】しかしながら、このようなパソコン上での電気的、デジタル的な記録によるものは容易に書き換えることができることから、記録媒体としての紙を用いて書かれた記録とは異なり、記録日時を含め記録内容を第

三者に証明することができないという問題を有していた。

【０００４】これに対し従来、デジタル文書に時刻印を押すサービスとして、特開平７－２５４８９７号公報に記載の「個人用日時認証装置」が知られる。この個人用日時認証装置は、スマートカード等に時刻認証装置を組込み、デジタル署名を行うときに時刻認証を一緒に行うものである。また、特開平３－１８５５５１号公報に記載の「デジタル時間認証装置」は、時刻認証装置を一つのハードウェアプラットフォームとして作成し、文書の作成者がその装置を使って時刻認証を行うものである。これらはいずれも、文書作成者が時刻認証を行う方式であるため、偽造がしやすく、第三者機関による証明でないため信頼性が乏しいものとなっている。

【０００５】また特開平６－１４０１８号公報に記載の「電子的公証方法および装置」は、元の文書に対するＣＲＣ（Cyclic Redundancy Check ；巡回冗長検査）、パリティ、検査合計を組み合わせて圧縮文書を作成し、時刻認証を行うものである。この方式で作成される圧縮文書は、現在広く暗号技術として使われているハッシュ関数（例えばＭＤ５やＳＨＡ－１など）を用いて作成する圧縮文書と比較して同一の圧縮文書をもつデジタル文書の偽造がしやすい。

【０００６】さらに特表平６－５０１５７１号公報に記載の「数値文書に確実にタイムスタンプを押す方法」は、時刻認証を行う外部機関が単独で時刻認証証明書を作成するものである。このタイムスタンプを押す方法は、外部機関が時刻認証証明書を偽造することが容易である。

【０００７】この欠点を補うために、受け取った時刻認証要求とその外部機関が直前に発行した時刻認証証明書を結合したデジタル文書に対してハッシュ関数を適用して得られた圧縮文書にデジタル署名を行い時刻認証証明書を作成する方法が提案されている。この方法は、時刻認証外部機関が時刻認証証明書を偽造することを事実上不可能にしているが、異なるラウンド（複数の時刻認証証明書を発行する一定期間）内での順序が正しい順序であるかどうかを検証することはできない。

【０００８】また、時刻認証証明書が真正であることを証明するためには、それ以前に発行した証明書が必要となる。すなわち、時刻認証外部機関が発行したすべての時刻認証証明書を保存するか、定期的に衆目にさらされたその時点での時刻認証証明書の値に辿り着くまでの時刻認証証明書を保存しておかないと、時刻認証証明書が真正であることを証明することができない。このため、システムとして膨大な記憶容量を必要とするとともに、真正であることの証明に膨大な時間を必要とする。

【０００９】現在、ＩＥＴＦ（Internet Engineering Task Force ）においてハッシュ関数により圧縮されたデジタル文書を外部機関に送付し、送付された圧縮デジタル文書に対して時刻認証証明書を作成するプロトコルの標準化が進められている。ここで標準化が検討されている方式においては、外部機関は１ヶ所で時刻認証証明書を作成するため、時刻認証証明書の偽造の可能性および時刻認証証明書を取得することが許されていない悪意のある第三者が不正に時刻認証証明書を取得する危険性を排除することができないという問題点をすでに含んでいる。

【００１０】

【発明が解決しようとする課題】一方、特願平１１－３５７６１号に記載の「時刻認証装置」では、時刻認証機関が単独でデジタル署名を作成するのではなく、公開鍵暗号における秘密鍵を分割したものに相当する部分秘密鍵を一つの時刻認証機関が所有し、第三者機関である各部分署名機関が独立に部分署名を作成することにより、時刻認証手段による時刻認証証明書の偽造を防止する手段を提供している。この時刻認証装置では、時刻認証手段を利用するクライアント側で、文書の作成履歴を定期的に作成し、その文書作成履歴に関する時刻認証証明書を時刻認証手段により作成することにより信頼性の高いデジタル文書の存在証明が可能となる。

【００１１】また、サーバ側では、時刻認証を行う外部機関が一つの秘密鍵を用いてデジタル署名を行う場合における秘密鍵の盗難の危険性やデジタル文書の著作者と時刻認証外部機関が結託して過去にさかのぼった時刻印を押す偽造の危険性を排除するために、時刻認証装置の秘密鍵を複数のデジタル署名手段が分割して持ち、それぞれのデジタル署名手段が独立してデジタル署名を行う。これにより秘密鍵盗難の危険性をなくするとともに、時刻を取得する手段とデジタル署名を行う手段を実行するすべての機関が結託しない限り時刻印を偽造することができないようにすることにより安全で信頼のおける時刻認証サービスを行う時刻認証外部機関を運営することができる。また、過去に発行した時刻認証証明書を一切保管する必要はなく、上述したような従来手法と比較して大幅に記憶容量を削減することが可能である。

【００１２】しかしながら、分散した時刻認証機関が部分秘密鍵を用いて同一のデジタル文書に時刻署名を独立に行う場合、全く同一の時刻を付けたデジタル文書にデジタル署名を行わないと、分散秘密鍵に対応する公開鍵でデジタル署名を検証することができない。

【００１３】本発明は、上記課題に鑑みてなされたもので、例えばパソコン上のデジタル文書に対して定期的に信頼のおける第三者機関から存在証明のための時刻認証証明書を取得しておくことにより、パソコン上のデジタル文書を研究ノートや家計簿と同様な日常的に履歴の残る記録とし、しかもその変更作成記録を第三者に証明することが可能な記録媒体として活用することができるフォルダ型時刻認証システムを提供することを目的とする。

【００１４】また、本発明は、独立に時刻署名を分散して行うときの複数の部分デジタル署名結果から得られる統合デジタル署名を一つの公開鍵を用いて復号し得るようにする分散時刻認証システムを提供することを目的とする。

【００１５】

【課題を解決するための手段】上記課題を解決するために、本発明は、クライアント装置とサーバ装置からなる時刻認証システムであって、クライアント装置は、複数のデジタル文書に対する複数のダイジェストを作成するダイジェスト作成手段と、このダイジェスト作成手段により作成された複数のダイジェストを結合するダイジェスト結合手段と、このダイジェスト結合手段により結合された複数のダイジェストから統合ダイジェストを作成する統合ダイジェスト作成手段と、この統合ダイジェスト作成手段により作成された統合ダイジェストを含んだ時刻認証要求をサーバ装置に送付する送付手段と、サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取る受取手段とを有し、サーバ装置は、時刻認証要求に応じて取得された時刻情報と統合ダイジェストを結合して求められた時刻印付きデジタル文書と、時刻印付きデジタル文書に対するデジタル署名とを含んだ時刻認証証明書を作成することを特徴とする時刻認証システムを提供する。

【００１６】また、本発明は、複数のデジタル文書に対する複数のダイジェストを作成するダイジェスト作成手段と、このダイジェスト作成手段により作成された複数のダイジェストを結合するダイジェスト結合手段と、このダイジェスト結合手段により結合された複数のダイジェストから統合ダイジェストを作成する統合ダイジェスト作成手段と、この統合ダイジェスト作成手段により作成された統合ダイジェストを含んだ時刻認証要求を時刻認証システムのサーバ装置に送付する送付手段と、サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取る受取手段と、を有することを特徴とする時刻認証システムのクライアント装置を提供する。

【００１７】また、本発明は、複数の時刻取得手段で、各時刻取得手段は、時刻認証要求に応じて、他の時刻取得手段とは独立に、所定の一定の刻み幅で与えられた前記時刻情報を順次取得する時刻取得手段と、これら複数の時刻取得手段に対応して設けられた複数の結合手段で、各結合手段は、他の結合手段とは独立に、対応する時刻取得手段により順次取得された時刻情報を統合ダイジェストを含んだデータを順次結合して複数の時刻印付きデジタル文書を作成する結合手段と、これら複数の結合手段に対応して設けられた複数のデジタル署名手段で、各デジタル署名手段は、他のデジタル署名手段とは独立に、対応する結合手段により作成された各時刻印付きデジタル文書に対するデジタル署名を生成するデジタル署名手段と、複数のデジタル署名手段によって生成された複数のデジタル署名から、複数のデジタル署名手段によって同一時刻の時刻印付きデジタル文書に対して生成された複数のデジタル署名を、各デジタル署名手段毎に一つずつ選択し、選択されたデジタル署名から統合デジタル署名を作成する統合デジタル署名作成手段と、この統合デジタル署名作成手段により作成された統合デジタル署名と前記同一時刻の時刻印付きデジタル文書から時刻認証証明書を作成する時刻認証証明書作成手段と、を有することを特徴とする時刻認証システムのサーバ装置を提供する。

【００１８】また、本発明は、クライアント装置とサーバ装置からなる時刻認証システムにおける時刻認証方法であって、（ａ）クライアント装置において、複数のデジタル文書に対する複数のダイジェストを作成するステップと、（ｂ）クライアント装置において、ステップ（ａ）により作成された複数のダイジェストを結合するステップと、（ｃ）クライアント装置のおいて、ステップ（ｂ）により結合された複数のダイジェストから統合ダイジェストを作成するステップと、（ｄ）ステップ（ｃ）により作成された統合ダイジェストを含んだ時刻認証要求をクライアント装置からサーバ装置に送付するステップと、（ｅ）サーバ装置において、時刻認証要求に応じて取得された時刻情報と統合ダイジェストを結合して求められた時刻印付きデジタル文書と、時刻印付きデジタル文書に対するデジタル署名とを含んだ時刻認証証明書を作成するステップと、（ｆ）クライアント装置において、サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取るステップと、を有することを特徴とする時刻認証方法を提供する。

【００１９】また、本発明は、時刻認証システムのクライアント装置において時刻認証サービスを受ける方法であって、（ａ）複数のデジタル文書に対する複数のダイジェストを作成するステップと、（ｂ）ステップ（ａ）により作成された複数のダイジェストを結合するステップと、（ｃ）ステップ（ｂ）により結合された複数のダイジェストから統合ダイジェストを作成するステップと、（ｄ）ステップ（ｃ）により作成された統合ダイジェストを含んだ時刻認証要求を時刻認証システムのサーバ装置に送付するステップと、（ｅ）サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取るステップと、を有することを特徴とする時刻認証サービスを受ける方法を提供する。

【００２０】また、本発明は、時刻認証システムのサーバ装置において時刻認証サービスを提供する方法であって、（ａ）サーバ装置の複数の時刻取得手段の各時刻取得手段において、時刻認証要求に応じて、他の時刻取得手段とは独立に、所定の一定の刻み幅で与えられた前記時刻情報を順次取得するステップと、（ｂ）サーバ装置のこれら複数の時刻取得手段に対応して設けられた複数の結合手段の各結合手段において、他の結合手段とは独

立に、対応する時刻取得手段により順次取得された時刻情報を統合ダイジェストを含んだデータを順次結合して複数の時刻印付きデジタル文書を作成するステップと、（ｃ）サーバ装置のこれら複数の結合手段に対応して設けられた複数のデジタル署名手段の各デジタル署名手段において、他のデジタル署名手段とは独立に、対応する結合手段により作成された各時刻印付きデジタル文書に対するデジタル署名を生成するステップと、（ｄ）複数のデジタル署名手段によって生成された複数のデジタル署名から、複数のデジタル署名手段によって同一時刻の時刻印付きデジタル文書に対して生成された複数のデジタル署名を、各デジタル署名手段毎に一つずつ選択し、選択されたデジタル署名から統合デジタル署名を作成するステップと、（ｅ）ステップ（ｄ）により作成された統合デジタル署名と前記同一時刻の時刻印付きデジタル文書から時刻認証証明書を作成するステップと、を有することを特徴とする時刻認証サービスを提供する方法を提供する。

【００２１】また、本発明は、コンピュータを時刻認証システムのクライアント装置として機能させるためのコンピュータ読み取り可能なプログラムコードを格納したコンピュータ利用可能な記録媒体であって、該コンピュータ読み取り可能なプログラムコードは、複数のデジタル文書に対する複数のダイジェストを作成する第一のプログラムコードと、この第一のプログラムコードにより作成された複数のダイジェストを結合する第二のプログラムコードと、この第二のプログラムコードにより結合された複数のダイジェストから統合ダイジェストを作成する第三のプログラムコードと、この第三のプログラムコードにより作成された統合ダイジェストを含んだ時刻認証要求を時刻認証システムのサーバ装置に送付する第四のプログラムコードと、サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取る第五のプログラムコードと、を有することを特徴とする記録媒体を提供する。

【００２２】また、本発明は、少なくとも一つのコンピュータを時刻認証システムのサーバ装置として機能させるためのコンピュータ読み取り可能なプログラムコードを格納したコンピュータ利用可能な記録媒体であって、該コンピュータ読み取り可能なプログラムコードは、複数の時刻取得手段で、各時刻取得手段は、時刻認証要求に応じて、他の時刻取得手段とは独立に、所定の一定の刻み幅で与えられた前記時刻情報を順次取得する時刻取得手段を実現するための第一のプログラムコードと、これら複数の時刻取得手段に対応して設けられた複数の結合手段で、各結合手段は、他の結合手段とは独立に、対応する時刻取得手段により順次取得された時刻情報を統合ダイジェストを含んだデータを順次結合して複数の時刻印付きデジタル文書を作成する結合手段を実現するための第二のプログラムコードと、これら複数の結合手段に対応して設けられた複数のデジタル署名手段で、各デジタル署名手段は、他のデジタル署名手段とは独立に、対応する結合手段により作成された各時刻印付きデジタル文書に対するデジタル署名を生成するデジタル署名手段を実現するための第三のプログラムコードと、複数のデジタル署名手段によって生成された複数のデジタル署名から、複数のデジタル署名手段によって同一時刻の時刻印付きデジタル文書に対して生成された複数のデジタル署名を、各デジタル署名手段毎に一つずつ選択し、選択されたデジタル署名から統合デジタル署名を作成す第四のプログラムコードと、この統合デジタル署名作成手段により作成された統合デジタル署名と前記同一時刻の時刻印付きデジタル文書から時刻認証証明書を作成する第五のプログラムコードと、を有することを特徴とする記録媒体を提供する。

【００２３】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。

【００２４】図１に本発明の第一の実施形態に係るフォルダ型時刻認証システムの構成を示す。

【００２５】図１において、フォルダ型時刻認証システム１は、テキスト情報、画像情報、音声情報が適宜、含まれるデジタル文書の内、対象となる対象デジタル文書Ｇのダイジェストを作成するダイジェスト作成手段１１と、このダイジェスト作成手段１１で作成される複数のダイジェストを結合するダイジェスト結合手段１３と、このダイジェスト結合手段１３で複数のダイジェストを結合して得られた全体の結果に対して統合ダイジェストを作成する統合ダイジェスト作成手段１５と、この統合ダイジェスト作成手段１５で作成された統合ダイジェストを含むデータを時刻認証手段２１を介してデジタル署名作成手段１９に送付する送付手段１７と、この送付手段１７を介して前記統合ダイジェスト作成手段１５から受け取った統合ダイジェストを含むデータに後述する時刻取得手段２３から取得した時刻を結合し、この結合した全体に対してデジタル署名を作成するデジタル署名作成手段１９と、これら各手段で作成され、取得された統合ダイジェスト、時刻、デジタル署名を含む時刻認証証明書を受取手段２５に送付する時刻認証手段２１と、この時刻認証手段２１により問い合わせのあった時点の時刻を時刻情報として提供する時刻取得手段２３と、前記時刻認証手段２１から送られる時刻認証証明書を受け取る受取手段２５により構成される。

【００２６】ここで、ダイジェスト作成手段１１と、ダイジェスト結合手段１３と、統合ダイジェスト作成手段１５と、送付手段１７と、受取手段２５がクライアント部１００を構成し、デジタル署名作成手段１９と時刻認証手段２１と時刻取得手段２３がサーバ部２００を構成する。

【００２７】以下、図１を参照して、第一の実施形態に

おける時刻認証処理について説明する。

【００２８】著作者により作成されたテキスト情報、画像情報、音声情報、バイナリ情報あるいはそれらの組み合わせからなる対象デジタル文書Ｇは、フォルダ型時刻認証システム１内のダイジェスト作成手段１１により、処理の高速化を計るとともに、サーバ部２００に元の文書を送付せずに済むようにし、しかも異なる文書に対して非常に高い確率で異なる値が得られるようにするために、各デジタル文書毎にハッシュ関数（例えばＳＨＡ－１やＭＤ５）を用いてダイジェストが作成される。

【００２９】具体的には、ハッシュ関数をｈ、対象デジタル文書Ｇを構成する複数のデジタル文書g_1，g_2，…，g_nとすると、ダイジェスト作成手段１１によりダイジェストｈ（g_1），ｈ（g_2），…，ｈ（g_n）が作成される。

【００３０】次に、ダイジェスト結合手段１３により、例えば、各ダイジェストｈ（g_1），ｈ（g_2），…，ｈ（g_n）を連接により結合した結果としてｈ（g_1）・ｈ（g_2）…ｈ（g_n）を得る。この結合結果から統合ダイジェスト作成手段１５により統合ダイジェストを作成する。

【００３１】ここで統合ダイジェスト作成手段１５で用いるハッシュ関数をｉとすると、ｉ（ｈ（g_1）・ｈ（g_2）…ｈ（g_n））が統合ダイジェストとなる。統合ダイジェストｉ（ｈ（g_1）・ｈ（g_2）…ｈ（g_n））を送付手段１７により時刻認証手段２１を介してデジタル署名作成手段１９に送付する。

【００３２】デジタル署名作成手段１９は、統合ダイジェストｉ（ｈ（g_1）・ｈ（g_2）…ｈ（g_n））と時刻取得手段２３により取得した時刻ｔを含むデジタルデータに対してデジタル署名ｓを作成し、このデジタル署名ｓを時刻認証手段２１に送出する。

【００３３】続いて、時刻認証手段２１では、このデジタル署名ｓと、統合ダイジェストｉ（ｈ（g_1）・ｈ（g_2）…ｈ（g_n））および時刻ｔを含む時刻認証証明書を発行し受取手段２５に送出する。

【００３４】第一の実施形態によれば、パソコン上のデジタル文書に対して定期的に信頼のおける第三者機関に存在証明のための時刻認証証明書を発行してもらうことにより、関連する文書や図、表などが一体となって一つの体系的な文書を構成することが多いデジタル文書においても、パソコン上のデジタル文書を、それらの関連文書あるいはそれらを作成しているパソコン上にある他のデジタル文書と関連付けて、時刻認証証明書を取得しておくことが可能となる。

【００３５】また、時刻認証を行った文書の存在証明の信頼性を向上することができ、さらにパソコン上のデジタル文書を研究ノートや家計簿と同様な日常的に履歴の残る記録とし、しかもその変更作成記録を第三者に証明することが可能な記録媒体として活用することができる。

【００３６】これにより、複数のデジタル文書が時刻印を押された時点以降において変更されてなく、かつ確かに時刻印が押された時点でこれら複数のデジタル文書が同時に存在していたことを証明することが可能となる。しかも、各デジタル文書毎に時刻認証証明書の要否を判定する必要がなく、複数のデジタル文書に対してまとめて一つの時刻認証証明書を取得すればよくなるため、時刻認証サービスを低コストで活用することが可能となる。

【００３７】次に、図２に本発明の第二の実施形態に係るフォルダ型時刻認証システムの構成を示す。

【００３８】図２において、フォルダ型時刻認証システム３は、テキスト文書、画像情報、音声情報が適宜、含まれるデジタル文書Ｆの内、対象となる対象デジタル文書Ｇのダイジェストを作成するダイジェスト作成手段３１と、このダイジェスト作成手段３１で作成される複数のダイジェストを結合するダイジェスト結合手段３３と、このダイジェスト結合手段３３で複数のダイジェストを結合して得られた全体の結果に対して統合ダイジェストを作成する統合ダイジェスト作成手段３５と、この統合ダイジェスト作成手段３５で作成された統合ダイジェストを含むデータを時刻認証手段４１を介してデジタル署名作成手段３９に送付する送付手段３７と、後述する時刻取得手段４３ａから取得した時刻を前記送付手段３７を介して統合ダイジェスト作成手段３５から受け取った統合ダイジェストを含むデータに結合し、この結合した全体に対してデジタル署名を作成するデジタル署名作成手段３９と、これら各手段で作成され、取得された統合ダイジェスト、時刻、デジタル署名を含む時刻認証証明書を受取手段４５に送付する時刻認証手段４１と、この時刻認証手段４１により問い合わせのあった時点の時刻を時刻情報として提供する時刻取得手段４３ａと、前記時刻認証手段４１から送られる時刻認証証明書を受け取る受取手段４５と、この受取手段４５を介して受けとった時刻認証証明書の検証を行う検証手段４７と、前記ダイジェスト作成手段３１に対し、ダイジェストの作成タイミングを指示する時刻指定手段４９と、デジタル文書Ｆから対象とするデジタル文書を指定するデジタル文書指定手段５１と、前記ダイジェスト作成手段３１、送付手段３７、受取手段４５および検証手段４７に対し問い合わせのあった時点の時刻を時刻情報として提供する時刻取得手段４３ｂにより構成される。なお、時刻取得手段４３ａと時刻取得手段４３ｂは、同一であっても構わない。

【００３９】ここで、ダイジェスト作成手段３１と、ダイジェスト結合手段３３と、統合ダイジェスト作成手段３５と、送付手段３７と、受取手段４５と、検証手段４７と、時刻指定手段４９と、デジタル文書指定手段５１と、時刻取得手段４３ｂがクライアント部１００を構成

し、デジタル署名作成手段３９と時刻認証手段４１と時刻取得手段４３ａがサーバ部２００を構成する。

【００４０】以下、図２を参照して、第二の実施形態における時刻認証処理について説明する。

【００４１】パソコン上からアクセス可能なパソコン内部あるいはネットワーク上のテキスト、音声、画像、バイナリ情報あるいはそれらの組み合わせからなるデジタル文書Ｆに対して、デジタル文書指定手段５１によりファイルまたはフォルダ単位で指定された対象デジタル文書Ｇを指定する。

【００４２】ダイジェスト作成手段３１が時刻取得手段４３ｂから取得した時刻に基づき時刻指定手段４９により指定された時刻になったことを検出したら、ダイジェスト作成手段３１は対象デジタル文書Ｇに対して、各デジタル文書毎にＳＨＡ－１やＭＤ５などのハッシュ関数を用いてダイジェストを作成する。

【００４３】ハッシュ関数をｈ、対象デジタル文書をg_1，g_2 …，g_n とすると、ダイジェスト作成手段３１によりダイジェストｈ（g_1 ），ｈ（g_2 ），…，ｈ（g_n ）が作成される。

【００４４】ダイジェスト結合手段３３により、例えば、ダイジェストｈ（g_1 ），ｈ（g_2 ），…，ｈ（g_n ）を連接により結合した結果ｈ（g_1 ）・ｈ（g_2 ）…ｈ（g_n ）を得る。結合結果から統合ダイジェスト作成手段３５により統合ダイジェストを作成する。

【００４５】統合ダイジェスト作成手段３５で用いるハッシュ関数をｉとすると、ｉ（ｈ（g_1 ）・ｈ（g_2 ）…ｈ（g_n ））が統合ダイジェストとなる。統合ダイジェストｉ（ｈ（g_1 ）・ｈ（g_2 ）…ｈ（g_n ））を送付手段３７により時刻認証手段４１を介してデジタル署名作成手段３９に送付する。

【００４６】デジタル署名作成手段３９は、統合ダイジェストｉ（ｈ（g_1 ）・ｈ（g_2 ）…ｈ（g_n ））と時刻取得手段４３ａにより取得した時刻ｔを含むデジタルデータに対して、デジタル署名ｓを作成し、このデジタル署名ｓを時刻認証手段４１に送出する。

【００４７】時刻認証手段４１は、統合ダイジェストｉ（ｈ（g_1 ）・ｈ（g_2 ）…ｈ（g_n ））、時刻ｔおよびデジタル署名ｓを含む時刻認証証明書を発行し受取手段４５に送出する。

【００４８】検証手段４７は、受取手段４５で受け取った時刻認証証明書についているデジタル署名がデジタル署名作成手段３９で作成された正しいデジタル署名であることを検証する。

【００４９】さらに、時刻認証証明書に付けられている時刻が送付手段３７がデジタル署名作成手段３９に送付した時刻以降であり、受取手段４５が受け取った時刻以前であることを検証する。

【００５０】上述したように、第二の実施形態によれば、第一の実施形態における効果に加え、さらにフォルダあるいはファイル単位で指定したパソコン上のファイルに対して定期的に時刻認証証明書を取得し、パソコン上のファイルの作成変更履歴を関連するファイルとの関係を含めて記録することができ、また長い時間に渡って取得した時刻認証証明書の系列はパソコン上のファイルの作成変更履歴に対する第三者による証明書とすることができる。この時刻認証証明書の系列は、研究ノートや家計簿以上に偽造が難しいため、デジタル文書に対して信頼性の高い時刻認証手段の提供が可能となる。

【００５１】なお、上述したこのようなフォルダ型時刻認証システム用のプログラムは記録媒体に記録して提供されることにより、該記録媒体を利用して、そのフォルダ型時刻認証プログラムの流通性を高めることができる。

【００５２】次に、図３に本発明の第三の実施形態に係る分散時刻認証システムの構成を示す。

【００５３】図３において、分散時刻認証システム１０１は、一定間隔をおいて少なくとも１回以上であるｎ回、各々独立にある一定の刻み幅の時刻情報t_1，t_2，…，t_n を取得する複数の時刻取得手段１１３ａ，１１３ｂ，・・・，１１３ｓと、これら時刻取得手段１１３ａ，１１３ｂ，・・・，１１３ｓ毎に１つずつ設けられ、デジタル文書Ｍに時刻情報t_i を結合して、各々独立に時刻印付きデジタル文書Mt_i を作成する、複数の結合手段１１１ａ，１１１ｂ，・・・，１１１ｓと、これら結合手段１１１ａ，１１１ｂ，・・・，１１１ｓ毎に１つずつ設けられ、各々独立にデジタル署名を作成する複数のデジタル署名手段１１５ａ，１１５ｂ，・・・，１１５ｓと、該複数のデジタル署名手段１１５ａ，１１５ｂ，・・・，１１５ｓで独立に作成された複数のデジタル署名を受け取り、これら複数のデジタル署名の中から互いに等しい時刻印付きデジタル文書Ｍｔから作成されたデジタル署名を各デジタル署名手段１１５ａ，１１５ｂ，・・・，１１５ｓ毎に１つ選択し、それらの選択された互いに等しい時刻印付きデジタル文書Ｍｔに対して、作成されたデジタル署名から統合デジタル署名ｃを作成する統合デジタル署名作成手段１１７と、これら時刻印付きデジタル文書Ｍｔおよび統合デジタル署名ｃを含む時刻認証証明書Ｔを作成する時刻認証証明書作成手段１１９により構成される。

【００５４】以下、図３を参照して第三の実施形態における分散時刻認証処理について説明する。ここでは結合手段１１１ａの系を中心に説明を進めるが、他の系においても同様である。

【００５５】著作者により作成されたテキスト文書、画像情報、音声情報、バイナリ情報あるいはそれらの組み合わせからなるデジタル文書Ｍから、分散時刻認証システム１０１内の結合手段１１１ａにおいて、時刻取得手段１１３ａにより取得された時刻と結合され時刻印付き

デジタル文書Ｍｔが作成される。この作成された時刻印付きデジタル文書Ｍｔに対するデジタル署名がデジタル署名手段１１５ａにより作成される。このように各デジタル署名手段１１５ａ，１１５ｂ，・・・，１１５ｓで作成されたデジタル署名は、統合デジタル署名作成手段１１７に集められる。

【００５６】さらに統合デジタル署名作成手段１１７は、共通の時刻を持つ時刻印付きデジタル文書Ｍｔがデジタル署名手段１１５毎に一つ選択することができるときには、それらの共通の時刻を持つ時刻印付きデジタル文書Ｍｔに対するデジタル署名から統合デジタル署名を作成する。続いて、時刻認証証明書作成手段１１９は、統合デジタル署名を作成するのに用いた時刻印付きデジタル文書Ｍｔと統合デジタル署名を含む時刻認証証明書Ｔを作成する。

【００５７】以下、デジタル署名作成について、一例をあげて説明する。なお、ここでは公開鍵暗号の具体例としてＲＳＡ公開鍵暗号を用いる。

【００５８】まず、ｐとｑを十分大きな素数とし、

$$n=pq$$

とおく。そして、

$$\phi(n)=(p-1)(q-1)$$

と互いに素な整数ｅを適当に定める。すなわち、

$$gcd(e,(p-1)(q-1))=1$$

そして、ｎとｅを公開鍵とし、ｄを

$$ed=1 \mod \phi(n)$$

である整数とするとき、ｐ，ｑ，ｄを秘密鍵とする。

【００５９】共通の時刻を持つ時刻印付きデジタル文書Ｍｔにハッシュ関数（例えばＳＨＡ－１やＭＤ５）を適用して得られるダイジェストをｍとする。

【００６０】さらに、

$$c=m^d \mod n$$

とおく。このとき、ｃを統合デジタル署名作成手段１１７により最終的に作成される統合デジタル署名とする。図３におけるデジタル署名手段１１５の総数をｓとしたとき、ｄを数の和で表現して

$$d=d_1+d_2+\cdots d_s$$

とおく。

【００６１】

$$c_1=m^{d_1} \mod n,\ \cdots,\ c_s=m^{d_s} \mod n$$

とすると、c_1，…，c_sがｓ個のデジタル署名手段１１５ａ，１１５ｂ，・・・，１１５ｓで作成されるデジタル署名となる。（Ｍｔ，ｃ）を含むデジタル文書が時刻認証証明書Ｔとなる。

【００６２】次に、図４に本発明の第四の実施形態に係る分散時刻認証システムの構成を示す。

【００６３】図４において、分散時刻認証システム１０３は、デジタル文書Ｍを通信により受け取る受取手段１３０と、一定間隔をおいて少なくとも１回以上であるｎ回、各々独立にある一定の刻み幅の時刻情報$t_{1,1}$，…，$t_{s,1}$を取得する複数の時刻取得手段１３３ａ，１３３ｂ，・・・，１３３ｓと、これら時刻取得手段１３３ａ，１３３ｂ，・・・，１３３ｓ毎に１つずつ設けられ、受取手段１３０で受けとったデジタル文書Ｍに時刻情報$t_{i,j}$を結合して、各々独立に時刻印付きデジタル文書$Mt_{i,j}$を作成する複数の結合手段１３１ａ，１３１ｂ，・・・，１３１ｓと、これら結合手段１３１ａ，１３１ｂ，・・・，１３１ｓ毎に１つずつ設けられ、各々独立にデジタル署名を作成する複数のデジタル署名手段１３５ａ，１３５ｂ，・・・，１３５ｓと、これら複数のデジタル署名手段１３５ａ，１３５ｂ，・・・，１３５ｓで独立に作成された複数のデジタル署名を受け取り、これら複数のデジタル署名の中から互いに等しい時刻印付きデジタル文書Ｍｔから作成されたデジタル署名を各デジタル署名手段１３５ａ，１３５ｂ，・・・，１３５ｓ毎に１つ選択し、それらの選択された互いに等しい時刻印付きデジタル文書Ｍｔに対して、作成されたデジタル署名から統合デジタル署名ｃを作成する統合デジタル署名作成手段１３７と、これら時刻印付きデジタル文書Ｍｔおよび統合デジタル署名ｃを含む時刻認証証明書Ｔを作成する時刻認証証明書作成手段１３９と、この時刻認証証明書作成手段１３９で作成された時刻認証証明書Ｔを通信によりデジタル文書の送付者に返送する送付手段１４１により構成される。

【００６４】図５および図６は、第三および第四の実施形態における取得時刻情報の関係を示す。ここでは、デジタル署名手段が３つある場合を例に取得時刻情報の関係を示している。図５および図６において、$t_{1,1}$，$t_{2,1}$，$t_{3,1}$は、３つの時刻取得手段が１回目に取得した時刻をそれぞれ表わし、$t_{1,2}$，$t_{2,2}$，$t_{3,2}$は、３つの時刻取得手段が２回目に取得した時刻をそれぞれ表わす。また、$t_{1,1}$，$t_{1,2}$，$t_{1,3}$は３つの時刻取得手段が第１回目に時刻取得を行ったときの正確な時刻をそれぞれ表し、$t_{j,1}$，$t_{j,2}$，$t_{j,3}$は３つの時刻取得手段が第２回目に時刻取得を行ったときの正確な時刻をそれぞれ表わす。

【００６５】図５では、３つの時刻取得手段とも１回目に同じ時刻情報を取得し、２回目も同じ時刻情報を取得したことを表わす。この場合には、$t_{1,1}=t_{2,1}=t_{3,1}$が統合デジタル署名の作成に用いられる時刻となる。同様に、図６では、第一、第二の時刻取得手段の２回目と、第三の時刻取得手段の１回目が同じ時刻情報を取得したことを表わす。この場合には、$t_{3,1}=t_{1,2}=t_{2,2}$が統合デジタル署名の作成に用いられる時刻となる。

【００６６】図７は、図６と比較して刻み幅を半分にした場合における時刻取得時の正確な時間と取得時刻情報の関係を示す。図７において、$t_{1,1}$，$t_{2,1}$，$t_{3,1}$は、３つの時刻取得手段が１回目に取得した時刻をそれぞれ表わし、$t_{1,2}$，$t_{2,2}$，$t_{3,2}$は、３つの時刻取

得手段が２回目に取得した時刻をそれぞれ表し、$t_{1,3}$，$t_{2,3}$，$t_{3,3}$は、３つの時刻取得手段が３回目に取得した時刻をそれぞれ表わす。また、$t_{1,1}$，$t_{1,2}$，$t_{1,3}$は３つの時刻取得手段が第１回目に時刻取得を行ったときの正確な時刻をそれぞれ表し、$t_{j,1}$，$t_{j,2}$，$t_{j,3}$は３つの時刻取得手段が第２回目に時刻取得を行ったときの正確な時刻をそれぞれ表し、$t_{k,1}$，$t_{k,2}$，$t_{k,3}$は３つの時刻取得手段が第３回目に時刻取得を行ったときの正確な時刻をそれぞれ表わす。この刻み幅を半分にした例では、３つの時刻取得手段により同じ時刻情報を取得するために、各時刻取得手段は少なくとも３回の時刻取得を行う必要がある。

【００６７】なお、各時刻取得手段が時刻取得を行う一定間隔は、任意の長さに設定可能であるが、各時刻取得手段が取得する時刻の一定の刻み幅と等しく設定することが好ましい。

【００６８】また、２回目以降の時刻取得を実際には行わずに、第１回目に取得した時刻に予め決められた一定の刻み幅の時間を順次加えて得られた時刻を２回目以降の取得時刻とすることも可能である。この場合には、各時刻取得手段は時刻取得を１回行うのみでよい。

【００６９】各時刻取得手段が取得する時刻の一定の刻み幅は、任意の長さに設定可能であるが、刻み幅を小さくすればするほど、取得される時刻の精度が向上する反面、共通の時刻を持つ時刻印付きデジタル文書Ｍｔがデジタル署名手段毎に一つ選択できるようになるまで各デジタル署名手段が作成することになるデジタル署名の数は増えることになる。

【００７０】但し、各結合手段にデジタル文書Ｍが到着する時間にばらつきがある場合には、以下のように、最も時間のかかる結合手段以外の結合手段に対応するデジタル署名手段において絶対に共通の時刻として使われることがない時刻の少なくとも一つに対するデジタル署名の作成は行わないようにして、デジタル署名の数を減らすことは可能である。

【００７１】図８は、異なる２つの結合手段にデジタル文書が到着する可能性のある時間幅の関係を表している。図８の（１）は、一方の結合手段にデジタル文書が最も遅く到着し得る時刻より後にしかもう一方の結合手段にデジタル文書が到着し得ない場合を表し、図８の（２）は、一方の結合手段にデジタル文書が最も遅く到着し得る時刻が、もう一方の結合手段にデジタル文書が到着する可能性のある時間帯の中に含まれ、かつ、前者の結合手段にデジタル文書が最も早く到着し得る時刻が後者の結合手段にデジタル文書が最も早く到着し得る時刻よりも前になる場合を表し、図８の（３）は、一方の結合手段にデジタル文書が到着する可能性のある時間帯が、もう一方の結合手段にデジタル文書が到着し得る時間帯に完全に含まれる場合を表す。任意の２つの結合手段に同じデジタル文書が到着する時間帯の関係はこれら３つのいずれかとなる。

【００７２】図９は、最も遅くデジタル文書が到着する結合手段への到着時間帯が時刻ｃとｄの間であり、それ以外の任意の結合手段にデジタル文書が到着する時間帯が時刻ａとｂの間である場合のａ，ｂ，ｃ，ｄの前後関係を表す。図９の（１），（２），（３）はそれぞれ図８の（１），（２），（３）に相当するケースを示す。ここで最も遅くデジタル文書が到着する結合手段をＣ１、それ以外の任意の結合手段をＣ２とする。また、刻み幅すなわちt_iとt_{i+1}の間隔をｕとする。

【００７３】ここで、一般に、各結合手段は現在時刻以降の直近の予め決められた時刻に、統合デジタル署名作成に絶対使われることがない時刻を除くために予め指定された０以上の時間を加えて得られた時刻を開始時刻として、予め指定された時間間隔で得られる指定個数の時間を時刻情報としてデジタル文書に結合することにより時刻印付きデジタル文書を作成するものとすることが可能である。

【００７４】ここで、予め指定された０以上の時間は、結合手段間でデジタル文書の到着時刻に固定的なずれがある場合に、本来は先に時刻印付きデジタル文書作成を開始する結合手段がそのずれに応じて時刻印付きデジタル文書作成の開始を遅らせるために使われる。

【００７５】また、指定個数は、結合手段におけるデジタル文書の到着時刻の時間幅に変動がありえる場合にも、必ず統合デジタル署名を作ることができるようにどのデジタル署名手段に対しても共通する時刻の時刻印付きデジタル文書が求められるようにするために使われる。

【００７６】図９の（１）の場合、（ｃ－ｂ）／ｕを越えない最大の整数値ｎとｕとの積をｖとし、時刻t_3とt_4の間の時刻ｅにデジタル文書がＣ２に到着したとすると、現在時刻はｅであり、ｎ＝１であるので、現在時刻以降の予め決められた時刻をt_4、予め指定された０以上の時間はｖ＝ｎ*ｕ＝１*ｕとすることが可能である。さらに、予め指定された時間間隔はｕであり、指定個数は（ｄ－ａ）／ｕ以上の最小の整数値ｍに１を加えてからｎを引いたた数とすることが可能である。この場合には、ｍ＝５であるから、指定個数は５＋１－１＝５となる。

【００７７】この結果、t_4を時刻情報とする時刻印付きデジタル文書は作成する必要がなく、t_4にｖを足して得られるt_5からの指定個数５個のt_5、t_6、t_7、t_8、t_9を時刻情報とする時刻印付きデジタル文書のみを作成すればよい。ｅがａとt_3の間にある場合には、同様にt_4、t_5、t_6、t_7、t_8を時刻情報とする時刻印付きデジタル文書のみを作成すればよい。ｅがt_4とｂの間にある場合には、同様にt_6、t_7、t_8、t_9、t_{10}を時刻情報とする時刻印付きデジタル文書のみを作成すればよい。

【００７８】図９の（２）の場合、時刻t_5とt_4の間の時刻ｅにデジタル文書がＣ２に到着したとすると、現在時刻はｅであり、現在時刻以降の予め決められた時刻をt_4、予め指定された０以上の時間は０とすることが可能である。さらに、予め指定された時間間隔はｕであり、指定個数は（ｄ－ａ）／ｕ以上の最小の整数値ｍに１を加えた数とすることが可能である。この場合には指定個数は６となるので、t_4、t_5、t_6、t_7、t_8、t_9を時間情報とする時刻印付きデジタル文書のみを作成することになる。

【００７９】図９の（３）の場合、時刻t_5とt_6の間の時刻ｅにデジタル文書がＣ２に到着したとすると、現在時刻はｅであり、現在時刻以降の予め決められた時刻をt_5、予め指定された０以上の時間は０とすることが可能である。さらに、予め指定された時間間隔はｕであり、指定個数は（ｄ－ａ）／ｕ以上の最小の整数値ｍに１を加えた数とすることが可能である。この場合には指定個数は３となるので、t_5、t_7、t_9を時間情報とする時刻付きデジタル文書のみを作成することになる。

【００８０】さて、通常、分散時刻認証システムにあっては、構成要素のデジタル署名手段が公開鍵暗号における秘密鍵の一部を分散して保持するので、秘密鍵の盗難や時刻認証証明書の偽造の危険性を小さくすることができるものの、前述したように時刻取得手段が各々独立に取得した時刻が一致する可能性は非常に小さいため統合デジタル署名を作成できないという問題がある。

【００８１】これに対し、第三、第四の実施形態では、上述してきたように、一定の刻み幅で時刻を取得するので、各々独立に取得した時刻が等しくなる可能性を高くできる。実際、図５および図６に示した例においては、一定間隔をおいて最低２回の時刻取得を各時刻取得手段毎に行えば、刻み幅と時刻取得手段間の時刻取得実行時間差の関係から必ず共通する時刻印付きデジタル文書をすべての結合手段で得ることが可能となる。この結果、秘密鍵の安全性を向上させる分散時刻署名が可能となる。

【００８２】このような分散時刻認証プログラムは記録媒体に記録して提供されることにより当該分散時刻認証プログラムの流通性を高めることができる。

【００８３】なお、上述した第三、第四の実施形態では、ＲＳＡを公開鍵暗号に用いた場合について説明したが、本発明はこれに限定されることなく楕円曲線公開鍵暗号、ＤＳＡ（Digital Signature Algorithm）等の秘密鍵を分割し、単一の秘密鍵で作成するデジタル署名と同じデジタル署名を、複数の分割した秘密鍵から作成することが可能な公開鍵暗号を用いても同様にデジタル署名および統合デジタル署名を作成することが可能である。

【００８４】また、時刻印付きデジタル文書Ｍｔの代わりに時刻印付きデジタル文書Ｍｔを含むデジタル文書を用いて統合デジタル署名を作成しても、何ら問題はない。さらにデジタル文書にハッシュ関数を適用せずに直接デジタル署名を作成することも可能である。また、１つの時刻印付きデジタル文書Ｍｔに１つの時刻情報を対応させるものであっても、１つの時刻印付きデジタル文書Ｍｔに複数の時刻情報を対応させるものであっても良い。つまり１つの時刻情報に対応する場合には１つの時刻印付きデジタル文書Ｍｔから１つのデジタル署名が作成され、複数の時刻情報に対応する場合には１つの時刻印付きデジタル文書Ｍｔから複数のデジタル署名が作成されることになる。

【００８５】次に、図１０に本発明の第五の実施形態に係るフォルダ型分散時刻認証システムの構成を示す。この第五の実施形態は、上述した第一および第二の実施形態と、第三および第四の実施形態とを組み合わせたものである。

【００８６】図１０において、フォルダ型分散時刻認証システム３００は、クライアント部１００とサーバ部２００からなる。クライアント部１００は時刻認証対象である複数のデジタル文書Ｇから時刻認証要求Ｒを作成し、サーバ部２００に渡す。サーバ部２００は、受け取った時刻認証要求Ｒに基いて時刻認証証明書Ｔを作成し、クライアント部１００に返す。

【００８７】図１１に、図１０のフォルダ型分散時刻認証システム３００におけるクライアント部１００の一構成例を示す。図１１のクライアント部１００は、上述した第二の実施形態における図２のクライアント部１００に相当するものであり、同一構成要素には同一符号を付してある。

【００８８】まず、デジタル文書指定手段５１により、デジタル文書の集合Ｆのなかから時刻認証の対象となるデジタル文書Ｇを選択する。

【００８９】次に、時刻指定手段４９が指定する定期的なダイジェスト作成時刻において、ダイジェスト作成手段３１により、選択されたデジタル文書毎にダイジェストを作成する。ここで前回ダイジェストを作成した後で内容に変更がないデジタル文書については前回作成したダイジェストを利用することも可能である。

【００９０】次に、ダイジェスト結合手段３３により、対象デジタル文書Ｇのそれぞれについてダイジェスト作成手段３１が作成したダイジェストを結合して一つの新たなデジタル文書を作成する。

【００９１】次に、統合ダイジェスト作成手段３６により、この新たなデジタル文書から統合ダイジェストを作成する。

【００９２】そして、統合ダイジェストを含む時刻認証要求Ｒを送付手段３７からサーバ部２００に送付する。

【００９３】サーバ部２００では、後述するように時刻認証証明書Ｔを作成し、クライアント部１００の受取手段４５に送付する。

25

【００９４】次に、検証手段４７が、送付手段３７による送付時刻と、受取手段４５による受取時刻と、受け取った時刻認証証明書Ｔに記録されている認証時刻を比較し、更に時刻認証証明書Ｔに含まれるデジタル署名がサーバ部２００により作成された真正なデジタル署名であることを、サーバ部２００が用いた秘密鍵に対応する公開鍵を用いて検証し、更に時刻認証証明書Ｔで時刻認証されているダイジェストが送付手段３７により送付されたものであるかどうか検証する。

【００９５】ここで、対象デジタル文書Ｇに前回の時刻認証証明書を含めることにより、対象デジタル文書Ｇの過去の作成、変更履歴を含めた時刻認証証明書を取得することが可能となる。

【００９６】図１２に、図１０のフォルダ型分散時刻認証システム３００におけるサーバ部２００の一構成例を示す。図１２のサーバ部２００は、上述した第四の実施形態における図４の分散時刻認証システムに相当するものであり、同一構成要素には同一符号を付してある。

【００９７】まず、受取手段１３０が時刻認証要求Ｒを受け取ると、そのコピーを各結合手段１３１に送る。

【００９８】次に、各結合手段１３１は、該当する時刻取得手段１３３により取得された時刻と時刻認証要求Ｒに含まれるデジタル文書Ｍを結合して時刻印付きデジタル文書Ｍｔを作成する。

【００９９】次に、この作成された時刻印付きデジタル文書Ｍｔに対するデジタル署名を、該当するデジタル署名手段１３５において予め取得している部分秘密鍵により作成する。このように各デジタル署名手段１３５で作成されたデジタル署名は、統合デジタル署名作成手段１３７に集められる。

【０１００】次に、統合デジタル署名作成手段１３７は、集められたデジタル署名のなかから、共通の時刻情報を持つデジタル署名を各デジタル署名手段１３５毎に一つ選択し、統合デジタル署名を作成する。

【０１０１】そして、時刻認証証明書作成手段１３９が、作成された統合デジタル署名を用いて時刻認証証明書Ｔを作成し、これを送付手段１４１からクライアント部１００に送付する。

【０１０２】図１３に、図１０のフォルダ型分散時刻認証システム３００におけるサーバ部２００の他の構成例を示す。図１３は、サーバ部２００の機能を独立した第三者機関により運用する分散配置構成を示すものであり、上述した図１２のサーバ部２００と同一構成要素には同一符号を付してある。

【０１０３】図１３においては、結合手段１３１、時刻取得手段１３３、デジタル署名手段１３５各一つずつの一組が一つの分散部分時刻認証機関２０５を構成し、受取手段１３０、統合デジタル署名作成手段１３７、時刻認証証明書作成手段１３９、送付手段１４１が一つの時刻認証機関２０４を構成している点が図１２と異なる

26

が、各手段の動作は図１２の場合と同じである。

【０１０４】

【発明の効果】上述したように、本発明のフォルダ型時刻認証システムによれば、パソコン上のデジタル文書に対して定期的に信頼のおける第三者機関から存在証明のための時刻認証証明書を取得しておくことにより日常的に履歴の残る記録とし、かつ変更作成記録を第三者に証明することが可能となる。

【０１０５】また、本発明の分散時刻認証システムによれば、必ず共通する時刻印付きデジタル文書をすべての結合手段で得ることが可能となるので、秘密鍵の安全性を向上させる分散時刻署名が可能となる。

【図面の簡単な説明】

【図１】本発明の第一の実施形態におけるフォルダ型時刻認証システムの構成例を示すブロック図。

【図２】本発明の第二の実施形態におけるフォルダ型時刻認証システムの構成例を示すブロック図。

【図３】本発明の第三の実施形態における分散時刻認証システムの構成例を示すブロック図。

【図４】本発明の第四の実施形態における分散時刻認証システムの構成例を示すブロック図。

【図５】図３および図４の分散時刻認証システムにおいて取得される取得時刻情報の一例を示す図。

【図６】図３および図４の分散時刻認証システムにおいて取得される取得時刻情報の他の例を示す図。

【図７】図３および図４の分散時刻認証システムにおいて取得される取得時刻情報の他の例を示す図。

【図８】図３および図４の分散時刻認証システムにおいて異なる２つの結合手段にデジタル文書が到着する可能性のある時間幅の関係を示す図。

【図９】図３および図４の分散時刻認証システムにおいて異なる２つの結合手段にデジタル文書が到着する可能性のある時間幅と到着時刻の例を示す図。

【図１０】本発明の第五の実施形態におけるフォルダ型分散時刻認証システムの構成例を示すブロック図。

【図１１】図１０のフォルダ型分散時刻認証システムにおけるクライアント部の一構成例を示すブロック図。

【図１２】図１０のフォルダ型分散時刻認証システムにおけるサーバ部の一構成例を示すブロック図。

【図１３】図１０のフォルダ型分散時刻認証システムにおけるサーバ部の他の構成例を示すブロック図。

【符号の説明】

１，３　フォルダ型時刻認証システム
１１，３１　ダイジェスト作成手段
１３，３３　ダイジェスト結合手段
１５，３５　統合ダイジェスト作成手段
１７，３７　送付手段
１９，３９　デジタル署名作成手段
２１，４１　時刻認証手段
２３，４３　時刻取得手段

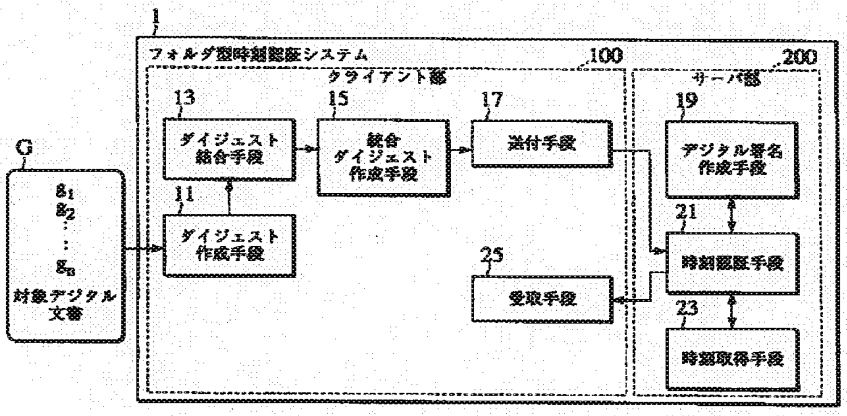
27

２５，４５　受取手段
４７　検証手段
４９　時刻指定手段
５１　デジタル文書指定手段
１００　クライアント部
１０１，１０３　分散時刻認証システム
１１１，１３１　結合手段
１１３，１３３　時刻取得手段
１１５，１３５　デジタル署名手段

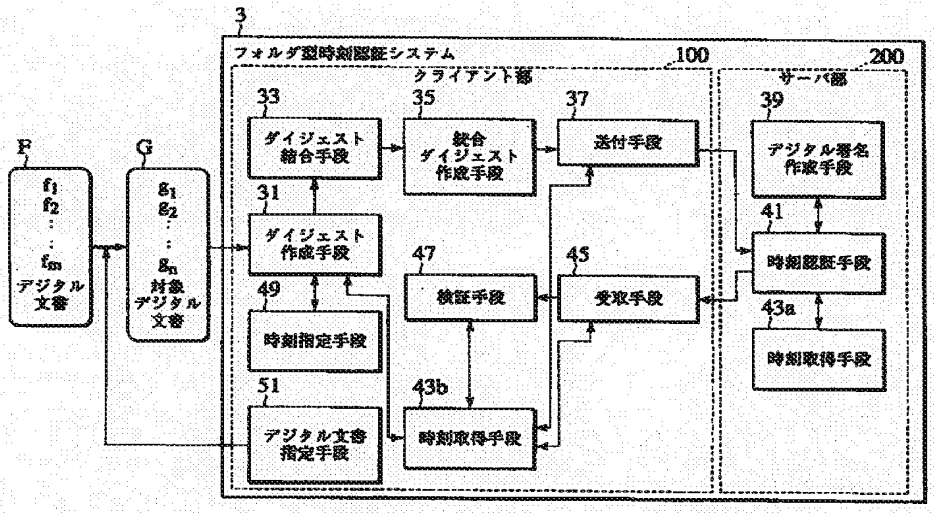
28

＊１１７，１３７　統合デジタル署名作成手段
１１９，１３９　時刻認証証明書作成手段
１３０　受取手段
１４１　送付手段
２００　サーバ部
３００　フォルダ型分散時刻認証システム
Ｍ　デジタル文書
Ｔ　時刻認証証明書
＊　Ｒ　時刻認証要求

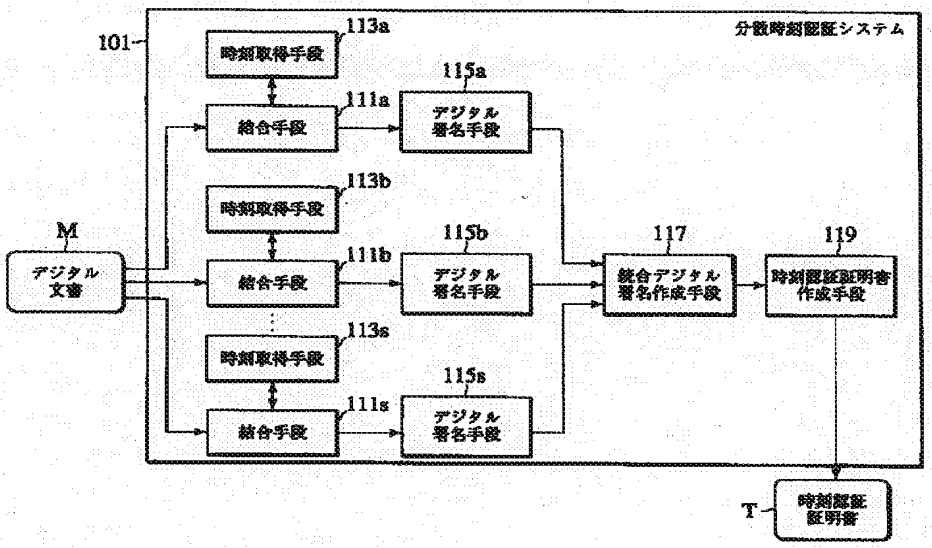
【図１】



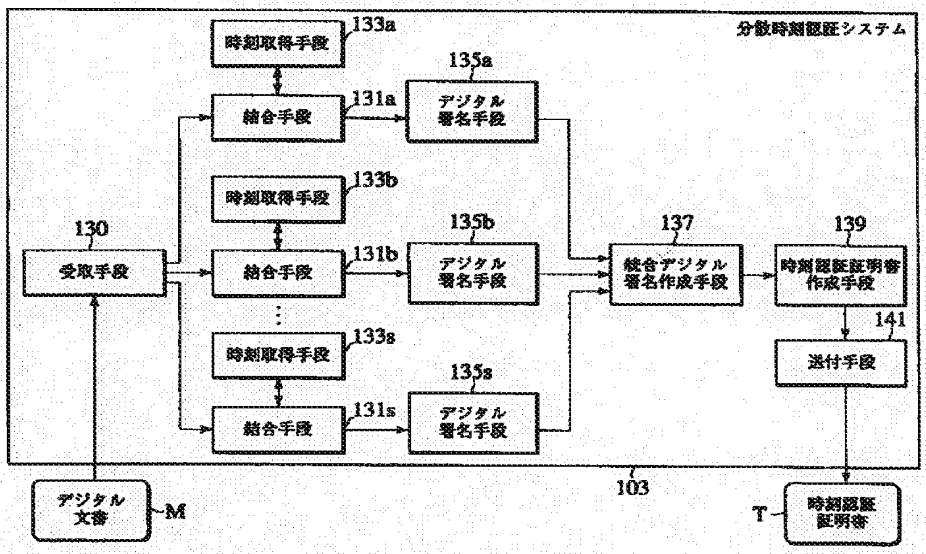
【図２】



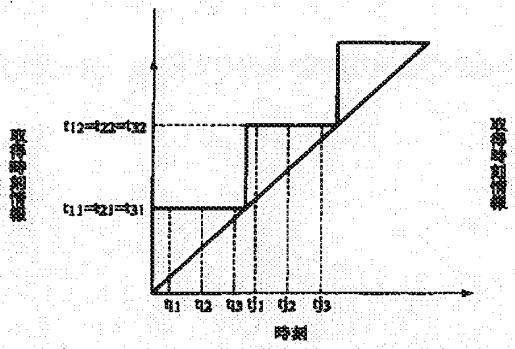
【図３】


101
分散時刻認証システム
時刻取得手段
113a
結合手段
111a
115a
デジタル署名手段
M
デジタル文書
113b
111b
115b
117
統合デジタル署名作成手段
119
時刻認証証明書作成手段
113s
111s
115s
T
時刻認証証明書

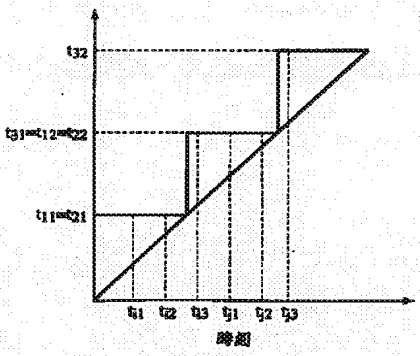
【図４】


分散時刻認証システム
時刻取得手段
133a
135a
結合手段
131a
デジタル署名手段
130
受取手段
133b
135b
131b
137
統合デジタル署名作成手段
139
時刻認証証明書作成手段
141
送付手段
133s
135s
131s
103
デジタル文書
M
T
時刻認証証明書

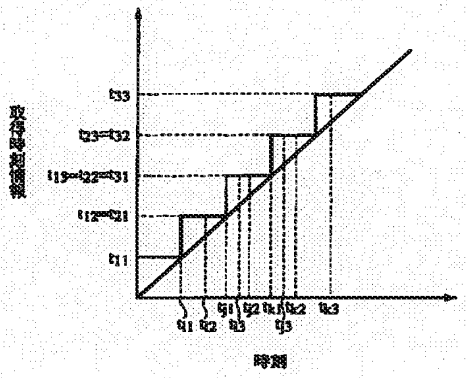
【図５】


t12=t22=t32
t11=t21=t31
t1 t2 t3 t1 t2 t3
時刻

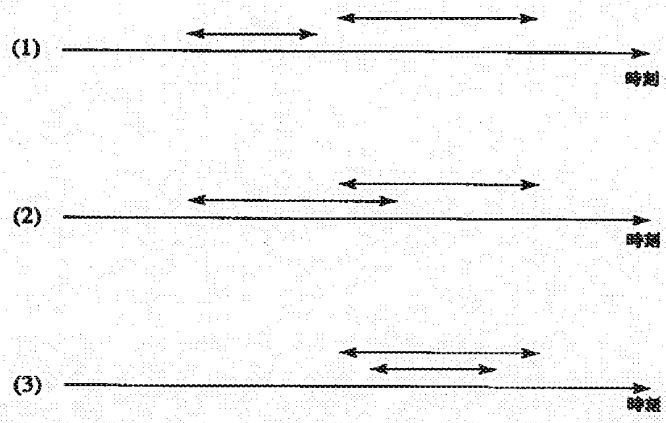
【図６】


t32
t31=t12=t22
t11=t21
t1 t2 t3 t1 t2 t3
時刻

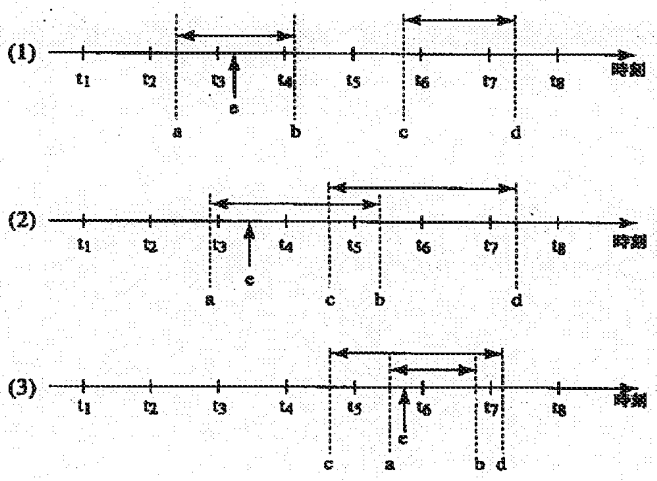
【図７】


t33
t23=t32
t13=t22=t31
t12=t21
t11
時刻

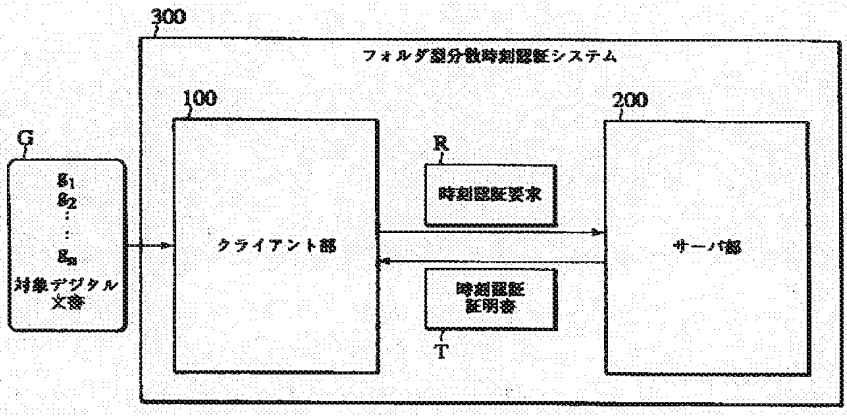
【図８】


(1)
時刻
(2)
時刻
(3)
時刻

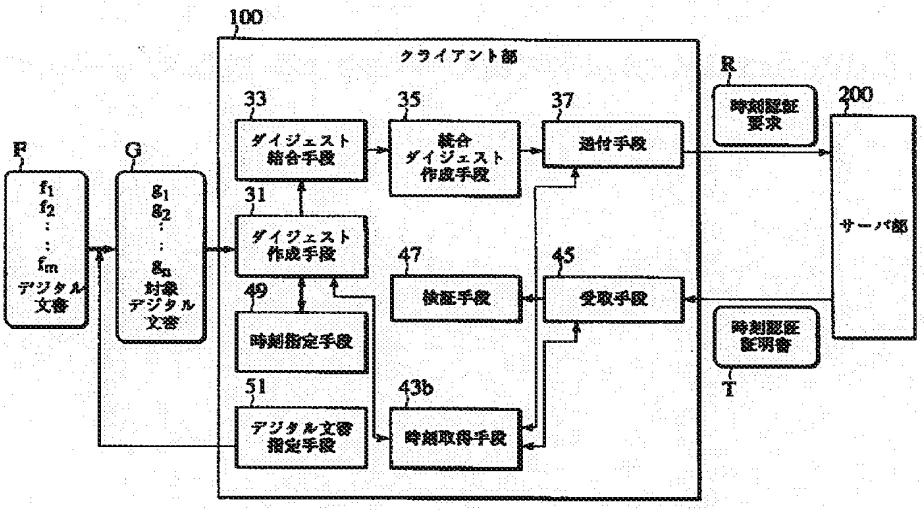
【図９】


(1)
t1 t2 t3 t4 t5 t6 t7 t8 時刻
e
a b c d
(2)
t1 t2 t3 t4 t5 t6 t7 t8 時刻
e
a c b d
(3)
t1 t2 t3 t4 t5 t6 t7 t8 時刻
e
c a b d

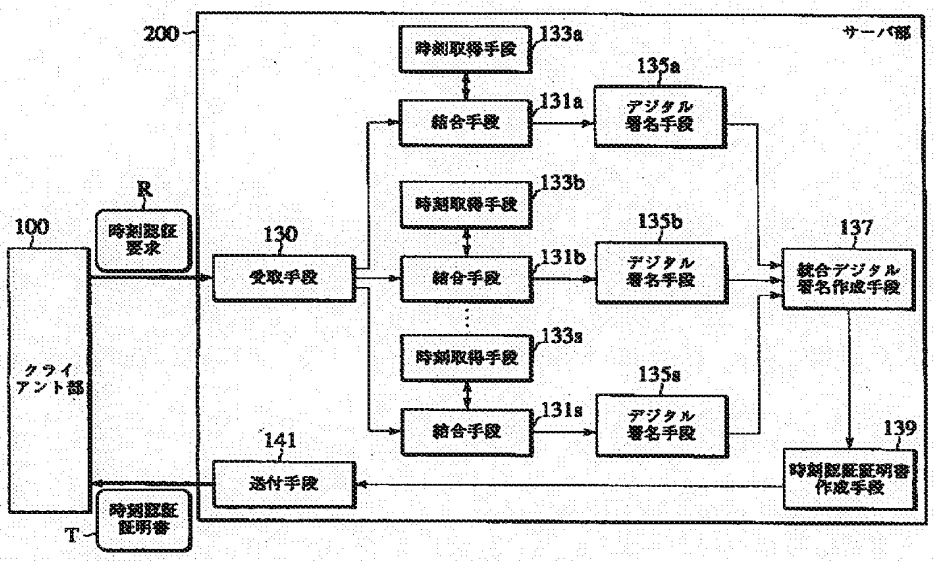
【図１０】


300
フォルダ型分散時刻認証システム
100
200
G
g_1
g_2
g_n
対象デジタル文書
クライアント部
R
時刻認証要求
時刻認証証明書
T
サーバ部

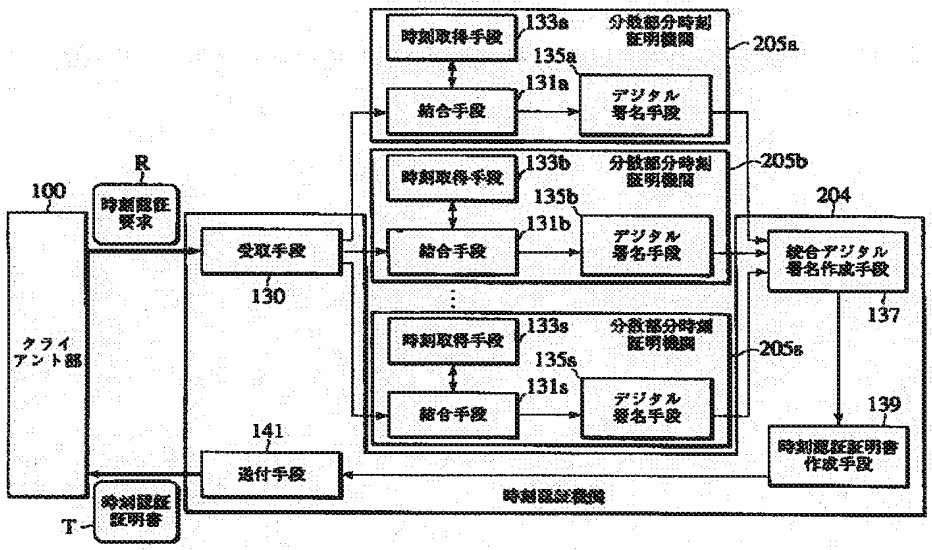
【図１１】


100
クライアント部
33
ダイジェスト結合手段
35
統合ダイジェスト作成手段
37
送付手段
31
ダイジェスト作成手段
47
検証手段
45
受取手段
49
時刻指定手段
51
デジタル文書指定手段
43b
時刻取得手段
F
f1 f2 ⋮ fm デジタル文書
G
g1 g2 ⋮ gn 対象デジタル文書
R
時刻認証要求
200
サーバ部
時刻認証証明書
T

【図１２】


200
サーバ部
時刻取得手段
133a
135a
結合手段
131a
デジタル署名手段
時刻取得手段
133b
135b
137
100
R
時刻認証要求
130
受取手段
結合手段
131b
デジタル署名手段
統合デジタル署名作成手段
時刻取得手段
133s
135s
クライアント部
結合手段
131s
デジタル署名手段
139
141
送付手段
時刻認証証明書作成手段
時刻認証証明書
T

【図１３】


100
クライアント部
R
時刻認証要求
受取手段
130
時刻取得手段
133a
分散部分時刻証明機関
205a
結合手段
135a
131a
デジタル署名手段
時刻取得手段
133b
分散部分時刻証明機関
205b
結合手段
135b
131b
デジタル署名手段
時刻取得手段
133s
分散部分時刻証明機関
205s
結合手段
135s
131s
デジタル署名手段
204
統合デジタル署名作成手段
137
139
時刻認証証明書作成手段
141
送付手段
時刻認証証明書
T
時刻認証機関

CLAIMS

[Claim(s)]
[Claim 1]A time stamp system which consists of a client apparatus and a server apparatus, comprising:
A digest preparing means which creates two or more digests in which a client apparatus receives two or more digital documents.
A digest coupling means which combines two or more digests created by this digest preparing means.
An integrated digest preparing means which creates an integrated digest from two or more digests combined by this digest coupling means.
An integrated digest created by this integrated digest preparing means.

[Claim 2]The time stamp system according to claim 1, wherein a client apparatus has further a digital document setting means which specifies said two or more digital documents per a file or folder from a digital document on a personal computer or a network.
[Claim 3]The time stamp system according to claim 2, wherein a digital document setting means specifies said two or more digital documents so that a time stamp certificate acquired before may be contained in said two or more digital documents.
[Claim 4]A client apparatus specifies periodical digest creation time as a digest preparing means further, The time stamp system according to claim 1 by which a digest preparing means is characterized by having a time designated means to create said two or more digests periodically at this periodical digest creation time.
[Claim 5]The time stamp system according to claim 1, wherein a client apparatus has

a verifying means which verifies whether a digital signature further contained in a time stamp certificate received by a receiving means is the right.
[Claim 6]The time stamp system comprising according to claim 1:
Sending time of a time stamp demand [in / in time when a client apparatus is shown with a digital document with a time seal further contained in a time stamp certificate received by a receiving means / a means of transmittal].
A verifying means which verifies that it is between receipt time of a time stamp certificate in a receiving means.

[Claim 7]The time stamp system comprising according to claim 1:
A digital signature means for a server apparatus to combine an integrated digest and time information, to ask for a digital document with a time seal, and to generate a digital signature to a digital document with a time seal.
A time stamp certificate preparing means which draws up a time stamp certificate from a digital document with a time seal generated by this digital signature means, and a digital signature.

[Claim 8]The time stamp system comprising according to claim 1:
A time acquiring means which acquires said time information to which server apparatus are two or more time acquiring means, and each time acquiring means was independently given by predetermined, fixed unit width with other time acquiring means according to a time stamp demand one by one.
A coupling means which each coupling means combines data which included an integrated digest for time information acquired one by one by corresponding time acquiring means independently of other coupling means one by one, and draws up two or more digital documents with a time seal by two or more coupling means established corresponding to a time acquiring means of these plurality.
A digital signature means to generate a digital signature to each digital document with a time seal which was drawn up by corresponding coupling means independently of other digital signature means by two or more digital signature means formed corresponding to a coupling means of these plurality as for each digital signature means.
From two or more digital signatures generated by two or more digital signature means. Two or more digital signatures generated to a digital document with a time seal of identical time by two or more digital signature means, An integrated-digital-signatures preparing means which chooses one at a time for every digital signature means, and

creates integrated digital signatures from a selected digital signature, A time stamp certificate preparing means which draws up a time stamp certificate from a digital document with a time seal of integrated digital signatures created by this integrated-digital-signatures preparing means and said identical time.

[Claim 9]The time stamp system according to claim 8, wherein each digital signature means is controlled not to generate a digital signature to at least one of the digital documents with a time seal of time which cannot turn into said identical time.
[Claim 10]The time stamp system according to claim 8, wherein an integrated-digital-signatures preparing means and a time stamp certificate preparing means constitute a time stamp organization and each class of a time acquiring means, a coupling means, and a digital signature means constitutes a distributed partial time stamp organization.
[Claim 11]A client apparatus of a time stamp system characterized by comprising the following.
A digest preparing means which creates two or more digests which receive two or more digital documents.
A digest coupling means which combines two or more digests created by this digest preparing means.
An integrated digest preparing means which creates an integrated digest from two or more digests combined by this digest coupling means.
A means of transmittal which sends a time stamp demand included an integrated digest created by this integrated digest preparing means to a server apparatus of a time stamp system, and a receiving means which receives a time stamp certificate to said two or more digital documents from a server apparatus.

[Claim 12]The client apparatus according to claim 11 having further a digital document setting means which specifies said two or more digital documents per a file or folder from a digital document on a personal computer or a network.
[Claim 13]The client apparatus according to claim 12, wherein a digital document setting means specifies said two or more digital documents so that a time stamp certificate acquired before may be contained in said two or more digital documents.
[Claim 14]The client apparatus according to claim 11 specifying periodical digest creation time as a digest preparing means, and having further a time designated means by which a digest preparing means creates said two or more digests periodically at this periodical digest creation time.

[Claim 15]The client apparatus according to claim 11 having further a verifying means which verifies whether a digital signature contained in a time stamp certificate received by a receiving means is the right.
[Claim 16]Sending time of a time stamp demand [in / in time shown with a digital document with a time seal contained in a time stamp certificate received by a receiving means / a means of transmittal], The client apparatus according to claim 11 having further a verifying means which verifies that it is between receipt time of a time stamp certificate in a receiving means.
[Claim 17]A server apparatus of a time stamp system characterized by comprising the following.
A time acquiring means which acquires said time information to which each time acquiring means was independently given by predetermined, fixed unit width with other time acquiring means by two or more time acquiring means according to a time stamp demand one by one.
A coupling means which each coupling means combines data which included an integrated digest for time information acquired one by one by corresponding time acquiring means independently of other coupling means one by one, and draws up two or more digital documents with a time seal by two or more coupling means established corresponding to a time acquiring means of these plurality.
A digital signature means to generate a digital signature to each digital document with a time seal which was drawn up by corresponding coupling means independently of other digital signature means by two or more digital signature means formed corresponding to a coupling means of these plurality as for each digital signature means.
From two or more digital signatures generated by two or more digital signature means. Two or more digital signatures generated to a digital document with a time seal of identical time by two or more digital signature means, An integrated-digital-signatures preparing means which chooses one at a time for every digital signature means, and creates integrated digital signatures from a selected digital signature, A time stamp certificate preparing means which draws up a time stamp certificate from a digital document with a time seal of integrated digital signatures created by this integrated-digital-signatures preparing means and said identical time.

[Claim 18]The server apparatus according to claim 17, wherein each digital signature means is controlled not to generate a digital signature to at least one of the digital documents with a time seal of time which cannot turn into said identical time.

[Claim 19]The server apparatus according to claim 17, wherein an integrated-digital-signatures preparing means and a time stamp certificate preparing means constitute a time stamp organization and each class of a time acquiring means, a coupling means, and a digital signature means constitutes a distributed partial time stamp organization.

[Claim 20]It is the time stamp method characterized by comprising the following in a time stamp system which consists of a client apparatus and a server apparatus, and is the (a) client apparatus.

A step which creates two or more digests which receive two or more digital documents.

(b) A step which combines two or more digests created by step (a) in a client apparatus.

(c) A step which creates an integrated digest from two or more digests which a client apparatus set and were combined by step (b).

(d) A step which sends a time stamp demand included an integrated digest created by step (c) to a server apparatus from a client apparatus.

(e) A digital document with a time seal which combined time information and an integrated digest which were acquired according to a time stamp demand, and was called for in a server apparatus.

A step which draws up a time stamp certificate having contained a digital signature to a digital document with a time seal.

(f) A step which receives a time stamp certificate to said two or more digital documents from a server apparatus in a client apparatus.

[Claim 21]A time stamp method according to claim 20 having further a step which specifies said two or more digital documents per a file or folder from a digital document on a personal computer or a network in a client apparatus.

[Claim 22]A time stamp method according to claim 21, wherein said step to specify specifies said two or more digital documents so that a time stamp certificate acquired before may be contained in said two or more digital documents.

[Claim 23]A time stamp method according to claim 20, wherein it specifies periodical digest creation time and a step (a) has further a step which creates said two or more digests periodically at this periodical digest creation time in a client apparatus.

[Claim 24]A time stamp method according to claim 20 having further a step which verifies whether a digital signature contained in a time stamp certificate received at a step (f) in a client apparatus is the right.

[Claim 25]Sending time of a time stamp demand [in / in time shown with a digital document with a time seal contained in a time stamp certificate received at a step (f) in a client apparatus / a step (d)], A time stamp method according to claim 20 having further a step which verifies that it is between receipt time of a time stamp certificate in a step (f).

[Claim 26]Said step (e) characterized by comprising the following is each time acquiring means of two or more time acquiring means of a server apparatus (e1).

A step which acquires said time information independently given by predetermined, fixed unit width with other time acquiring means one by one according to a time stamp demand.

(e2) In each coupling means of two or more coupling means established corresponding to a time acquiring means of these plurality of a server apparatus, A step which combines data which included an integrated digest for time information acquired one by one by corresponding time acquiring means independently of other coupling means one by one, and draws up two or more digital documents with a time seal.

(e3) A step which generates a digital signature to each digital document with a time seal drawn up by corresponding coupling means independently of other digital signature means in each digital signature means of two or more digital signature means formed corresponding to a coupling means of these plurality of a server apparatus.

(e4) From two or more digital signatures generated by two or more digital signature means. Two or more digital signatures generated to a digital document with a time seal of identical time by two or more digital signature means, A step which chooses one at a time for every digital signature means, and creates integrated digital signatures from a selected digital signature, and integrated digital signatures created by step (e5) (e4) and a step which draws up a time stamp certificate from a digital document with a time seal of said identical time.

[Claim 27]A time stamp method according to claim 26, wherein each digital signature means is controlled in said step (e3) not to generate a digital signature to at least one of the digital documents with a time seal of time which cannot turn into said identical time.

[Claim 28]A method characterized by comprising the following of receiving time stamp service in a client apparatus of a time stamp system.

(a) A step which creates two or more digests which receive two or more digital documents.

(b) A step which combines two or more digests created by step (a).
(c) A step which creates an integrated digest from two or more digests combined by step (b).
(d) A step which sends a time stamp demand included an integrated digest created by step (c) to a server apparatus of a time stamp system, and a step which receives a time stamp certificate to said two or more digital documents from the (e) server apparatus.

[Claim 29]How to receive the time stamp service according to claim 28 having further a step which specifies said two or more digital documents per a file or folder from a digital document on a personal computer or a network.
[Claim 30]How to receive the time stamp service according to claim 29, wherein said step to specify specifies said two or more digital documents so that a time stamp certificate acquired before may be contained in said two or more digital documents.
[Claim 31]How to receive the time stamp service according to claim 28 specifying periodical digest creation time and having further a step to which a step (a) creates said two or more digests periodically at this periodical digest creation time in a client apparatus.
[Claim 32]A digital document with a time seal which a time stamp certificate combined time information and an integrated digest which were acquired according to a time stamp demand, and was called for, In [a digital signature to a digital document with a time seal is included, and] a client apparatus, How to receive the time stamp service according to claim 28 having further a step which verifies whether a digital signature contained in a time stamp certificate received at a step (e) is the right.
[Claim 33]A digital document with a time seal which a time stamp certificate combined time information and an integrated digest which were acquired according to a time stamp demand, and was called for, In [a digital signature to a digital document with a time seal is included, and] a client apparatus, Sending time of a time stamp demand [in / in time shown with a digital document with a time seal contained in a time stamp certificate received at a step (e) / a step (d)], How to receive the time stamp service according to claim 28 having further a step which verifies that it is between receipt time of a time stamp certificate in a step (e).
[Claim 34]It is a method characterized by comprising the following of providing time stamp service in a server apparatus of a time stamp system, and is each time acquiring means of two or more time acquiring means of the (a) server apparatus.
A step which acquires said time information independently given by predetermined,

fixed unit width with other time acquiring means one by one according to a time stamp demand.
(b) In each coupling means of two or more coupling means established corresponding to a time acquiring means of these plurality of a server apparatus, A step which combines data which included an integrated digest for time information acquired one by one by corresponding time acquiring means independently of other coupling means one by one, and draws up two or more digital documents with a time seal.
(c) A step which generates a digital signature to each digital document with a time seal drawn up by corresponding coupling means independently of other digital signature means in each digital signature means of two or more digital signature means formed corresponding to a coupling means of these plurality of a server apparatus.
(d) From two or more digital signatures generated by two or more digital signature means. Two or more digital signatures generated to a digital document with a time seal of identical time by two or more digital signature means, A step which chooses one at a time for every digital signature means, and creates integrated digital signatures from a selected digital signature, and integrated digital signatures created by the (e) step (d) and a step which draws up a time stamp certificate from a digital document with a time seal of said identical time.

[Claim 35]How to provide the time stamp service according to claim 34, wherein each digital signature means is controlled in said step (c) not to generate a digital signature to at least one of the digital documents with a time seal of time which cannot turn into said identical time.
[Claim 36]A recording medium characterized by comprising the following which stored a program code in which computer reading for operating a computer as a client apparatus of a time stamp system is possible and in which computer applications are possible.
The first program code with which a program code in which this computer reading is possible creates two or more digests which receive two or more digital documents.
The second program code that combines two or more digests created by this first program code.
The third program code that creates an integrated digest from two or more digests combined by this second program code.
The fourth program code that sends a time stamp demand included an integrated digest created by this third program code to a server apparatus of a time stamp

system, and the fifth program code that receives a time stamp certificate to said two or more digital documents from a server apparatus.

[Claim 37]A recording medium characterized by comprising the following which stored a program code in which computer reading for operating at least one computer as a server apparatus of a time stamp system is possible and in which computer applications are possible.
The first program code for program codes in which this computer reading is possible to be two or more time acquiring means, and for each time acquiring means realize a time acquiring means which acquires said time information independently given by predetermined, fixed unit width with other time acquiring means one by one according to a time stamp demand.
Corresponding to a time acquiring means of these plurality, by two or more established coupling means, each coupling means, The second program code for realizing a coupling means which combines data which included an integrated digest for time information acquired one by one by corresponding time acquiring means independently of other coupling means one by one, and draws up two or more digital documents with a time seal.
Corresponding to a coupling means of these plurality, by two or more formed digital signature means, each digital signature means, The third program code for realizing a digital signature means to generate a digital signature to each digital document with a time seal drawn up by corresponding coupling means independently of other digital signature means.
From two or more digital signatures generated by two or more digital signature means. Two or more digital signatures generated to a digital document with a time seal of identical time by two or more digital signature means, Choose one at a time for every digital signature means, and integrated digital signatures from a selected digital signature The fourth program code of ******, Integrated digital signatures created by this integrated-digital-signatures preparing means and the fifth program code that draws up a time stamp certificate from a digital document with a time seal of said identical time.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]In the service which pushes a time seal, this invention is not changed into a digital document after the time of a digital document having a time seal pushed, And when surely a time seal is pushed, it is related with the folder type time stamp system and distributed time stamp system which make it possible to prove that the target digital document existed.

[0002]

[Description of the Prior Art]For example, under the patent system based on the first-to-invent rule in the U.S., it is known that it will be possible to use as a proof the research note containing the date proves a right of priority to be, and the housekeeping book in which the date was attached further can be used as expenditure record in a final declaration. On the other hand, it is becoming very general to perform everyday record of a research note, a housekeeping book, etc. using a personal computer as a personal computer comes to be used daily.

[0003]However, since what is depended on electric and the digital record on such a personal computer was rewritten easily, unlike the record written using the paper as a recording medium, it had the problem that the contents of record including a recording date could not be proved for a third party.

[0004]On the other hand, "the personal time authentication device" of a statement is conventionally known by JP,7-254897,A as service which stamps a time seal on a digital document. This personal time authentication device builds a time stamp device into a smart card etc., and when performing a digital signature, it performs a time stamp together. A "digital time authentication device" given in JP,3-185551,A creates a time stamp device as one hardware platform, and the maker of a document performs a time stamp using the device. Since each of these is methods with which a document preparation person performs a time stamp, they tends to carry out forgery, and since they is not the proof by an independent organization, they is what has scarce reliability.

[0005]"The electronic authentication method and a device" given in JP,6-14018,A draw up a compression document combining CRC (Cyclic Redundancy Check; Cyclic Redundancy Check), the parity, and the checksum to the original document, and perform a time stamp. The compression document drawn up by this method tends to

carry out forgery of the digital document which has the same compression document as compared with the compression document drawn up using the hash functions (for example, MD5, SHA-1, etc.) widely used as encoding technology now.

[0006]Furthermore, the outside facilities to which "the method of pushing a time stamp on a numerical document certainly" given in the Patent Publication Heisei No. 501571 [six to] gazette performs a time stamp draw up a time stamp certificate independently. The method of pushing this time stamp is easy for outside facilities to forge a time stamp certificate.

[0007]In order to compensate this fault, the method of performing a digital signature in the compression document obtained with the application of the hash function to the digital document which combined the time stamp certificate which the received time stamp demand and its outside facilities published immediately before, and drawing up a time stamp certificate is proposed. Although this method makes it impossible that time stamp outside facilities forge a time stamp certificate as a matter of fact, it cannot verify whether an order within a different round (fixed time which publishes two or more time stamp certificates) is a right order.

[0008]In order to prove that a time stamp certificate is genuine, the certificate published before it is needed. That is, unless it saves a time stamp certificate until it arrives at the value of the time stamp certificate in the time of saving all the time stamp certificates which time stamp outside facilities published, or being periodically exposed to public attention, it cannot prove that a time stamp certificate is genuine. For this reason, while needing a storage capacity huge as a system, huge time is needed for the proof of a genuine thing.

[0009]Now, standardization of the protocol which sends the digital document compressed by the hash function in IETF (Internet Engineering Task Force) to outside facilities, and draws up a time stamp certificate to the sent compression digital document is advanced. In the method with which standardization is considered here, Outside facilities have already included the problem that the danger that a third party with the bad faith which is not allowed to acquire the possibility and the time stamp certificate of forgery of a time stamp certificate will acquire a time stamp certificate unjustly cannot be eliminated in order to draw up a time stamp certificate at one place.

[0010]

[Problem(s) to be Solved by the Invention]On the other hand, with the "time stamp device" of a statement. [Japanese Patent Application No. / No. 35761 / 11 to] A time stamp organization does not create a digital signature independently, but one time stamp organization owns the partial secret key equivalent to what divided the

secret key in public key encryption, When each partial sign organization which is an independent organization creates a partial sign independently, a means to prevent forgery of the time stamp certificate by a time stamp means is provided. In this time stamp device, the existence proof of a reliable digital document becomes possible by creating the creation history of a document periodically and drawing up the time stamp certificate about that document preparation history by a time stamp means by the client side using a time stamp means.

[0011]In order to eliminate the danger of the forgery which pushes the time seal which the danger of the theft of a secret key and the author of a digital document in case the outside facilities which perform a time stamp perform a digital signature in the server side using one secret key, and time stamp outside facilities conspired, and went back in the past, Two or more digital signature means divide and have a secret key of a time stamp device, and each digital signature means performs a digital signature independently. While this abolishes the danger of a secret key theft, Unless all the organizations that perform a means to acquire time, and a means to perform a digital signature conspire, by preventing from forging a time seal, it is safe and the time stamp outside facilities which offer time stamp service which can set reliance can be managed. It is possible to reduce a storage capacity substantially as compared with conventional method which does not need to keep any time stamp certificate published in the past, and mentioned it above.

[0012]However, when the dispersed time stamp organization performs a time signature in the same digital document independently using a partial secret key, unless it performs a digital signature in the digital document which attached the same time at all, a digital signature is unverifiable by the public key corresponding to a distributed secret key.

[0013]This invention by in light of the above-mentioned problems acquiring the time stamp certificate for existence proof from the independent organization which can set reliance periodically, for example to the digital document on a personal computer, The digital document on a personal computer is considered as the same record as a research note or a housekeeping book in which a history remains daily, and it aims at providing a folder type time stamp system utilizable as a recording medium which can moreover prove the change creation record for a third party.

[0014]An object of this invention is to provide the distributed time stamp system which enables it to decode the integrated digital signatures obtained from two or more partial digital signature results when performing a time signature dispersedly independently using one public key.

[0015]
[Means for Solving the Problem]In order to solve an aforementioned problem, this invention is a time stamp system which consists of a client apparatus and a server apparatus, and a client apparatus, A digest preparing means which creates two or more digests which receive two or more digital documents, A digest coupling means which combines two or more digests created by this digest preparing means, An integrated digest preparing means which creates an integrated digest from two or more digests combined by this digest coupling means, A means of transmittal which sends a time stamp demand included an integrated digest created by this integrated digest preparing means to a server apparatus, Have a receiving means which receives a time stamp certificate to said two or more digital documents from a server apparatus, and a server apparatus, A time stamp system drawing up a time stamp certificate having contained a digital document with a time seal which combined time information and an integrated digest which were acquired according to a time stamp demand, and was called for, and a digital signature to a digital document with a time seal is provided.
[0016]A digest preparing means which creates two or more digests in which this invention receives two or more digital documents, A digest coupling means which combines two or more digests created by this digest preparing means, An integrated digest preparing means which creates an integrated digest from two or more digests combined by this digest coupling means, A means of transmittal which sends a time stamp demand included an integrated digest created by this integrated digest preparing means to a server apparatus of a time stamp system, A client apparatus of a time stamp system having a receiving means which receives a time stamp certificate to said two or more digital documents from a server apparatus is provided.
[0017]This inventions are two or more time acquiring means, and each time acquiring means, They are a time acquiring means which acquires said time information to which other time acquiring means were independently given by predetermined, fixed unit width according to a time stamp demand one by one, and two or more coupling means established corresponding to a time acquiring means of these plurality, A coupling means which each coupling means combines data which included an integrated digest for time information acquired one by one by corresponding time acquiring means independently of other coupling means one by one, and draws up two or more digital documents with a time seal, Corresponding to a coupling means of these plurality, by two or more formed digital signature means, each digital signature means, A digital signature means to generate a digital signature to each digital document with a time

seal drawn up by corresponding coupling means independently of other digital signature means, From two or more digital signatures generated by two or more digital signature means. An integrated-digital-signatures preparing means which chooses two or more one digital signatures of every generated to a digital document with a time seal of identical time by two or more digital signature means for every digital signature means, and creates integrated digital signatures from a selected digital signature, A server apparatus of a time stamp system having integrated digital signatures created by this integrated-digital-signatures preparing means and a time stamp certificate preparing means which draws up a time stamp certificate from a digital document with a time seal of said identical time is provided.

[0018]In [this invention is the time stamp method in a time stamp system which consists of a client apparatus and a server apparatus, and] the (a) client apparatus, In a step which creates two or more digests which receive two or more digital documents, and the (b) client apparatus, A step which combines two or more digests created by step (a), (c) A step which creates an integrated digest from two or more digests which a client apparatus set and were combined by step (b), (d) In a step which sends a time stamp demand included an integrated digest created by step (c) to a server apparatus from a client apparatus, and the (e) server apparatus, A digital document with a time seal which combined time information and an integrated digest which were acquired according to a time stamp demand, and was called for, A time stamp method having a step which draws up a time stamp certificate having contained a digital signature to a digital document with a time seal, and a step which receives a time stamp certificate to said two or more digital documents from a server apparatus in the (f) client apparatus is provided.

[0019]A step which creates two or more digests which this invention is the method of receiving time stamp service in a client apparatus of a time stamp system, and receive a digital document of (a) plurality, (b) A step which combines two or more digests created by step (a), (c) A step which creates an integrated digest from two or more digests combined by step (b), (d) A step which sends a time stamp demand included an integrated digest created by step (c) to a server apparatus of a time stamp system, (e) Provide a method of receiving time stamp service having a step which receives a time stamp certificate to said two or more digital documents from a server apparatus.

[0020]In [this invention is the method of providing time stamp service in a server apparatus of a time stamp system, and] each time acquiring means of two or more time acquiring means of the (a) server apparatus, A step which acquires said time information independently given by predetermined, fixed unit width with other time

acquiring means one by one according to a time stamp demand, (b) In each coupling means of two or more coupling means established corresponding to a time acquiring means of these plurality of a server apparatus, A step which combines data which included an integrated digest for time information acquired one by one by corresponding time acquiring means independently of other coupling means one by one, and draws up two or more digital documents with a time seal, (c) In each digital signature means of two or more digital signature means formed corresponding to a coupling means of these plurality of a server apparatus, A step which generates a digital signature to each digital document with a time seal drawn up by corresponding coupling means independently of other digital signature means, (d) Choose two or more one digital signatures of every per digital signature means generated to a digital document with a time seal of identical time by two or more digital signature means from two or more digital signatures generated by two or more digital signature means, A step which creates integrated digital signatures from a selected digital signature, (e) Provide a method of providing time stamp service having integrated digital signatures created by step (d) and a step which draws up a time stamp certificate from a digital document with a time seal of said identical time.

[0021]This invention is a recording medium which stored a program code in which computer reading for operating a computer as a client apparatus of a time stamp system is possible and in which computer applications are possible, A program code in which this computer reading is possible, The first program code that creates two or more digests which receive two or more digital documents, The second program code that combines two or more digests created by this first program code, The third program code that creates an integrated digest from two or more digests combined by this second program code, The fourth program code that sends a time stamp demand included an integrated digest created by this third program code to a server apparatus of a time stamp system, A recording medium having the fifth program code that receives a time stamp certificate to said two or more digital documents from a server apparatus is provided.

[0022]This invention is a recording medium which stored a program code in which computer reading for operating at least one computer as a server apparatus of a time stamp system is possible and in which computer applications are possible, A program code in which this computer reading is possible, The first program code for each time acquiring means to realize a time acquiring means which acquires said time information independently given by predetermined, fixed unit width with other time acquiring means one by one by two or more time acquiring means according to a time

stamp demand, Corresponding to a time acquiring means of these plurality, by two or more established coupling means, each coupling means, The second program code for realizing a coupling means which combines data which included an integrated digest for time information acquired one by one by corresponding time acquiring means independently of other coupling means one by one, and draws up two or more digital documents with a time seal, Corresponding to a coupling means of these plurality, by two or more formed digital signature means, each digital signature means, The third program code for realizing a digital signature means to generate a digital signature to each digital document with a time seal drawn up by corresponding coupling means independently of other digital signature means, From two or more digital signatures generated by two or more digital signature means. Two or more digital signatures generated to a digital document with a time seal of identical time by two or more digital signature means, Choose one at a time for every digital signature means, and integrated digital signatures from a selected digital signature The fourth program code of ******, A recording medium having integrated digital signatures created by this integrated-digital-signatures preparing means and the fifth program code that draws up a time stamp certificate from a digital document with a time seal of said identical time is provided.

[0023]

[Embodiment of the Invention]Hereafter, an embodiment of the invention is described using a drawing.

[0024]The composition of the folder type time stamp system concerning a first embodiment of this invention is shown in drawing 1.

[0025]In drawing 1, the folder type time stamp system 1, The digest preparing means 11 in which text information, picture information, and speech information create the digest of the target object digital document G among the digital documents contained suitably, The digest coupling means 13 which combines two or more digests created by this digest preparing means 11, The integrated digest preparing means 15 which creates an integrated digest to the result of the whole produced by combining two or more digests by this digest coupling means 13, The means of transmittal 17 which sends data including the integrated digest created by this integrated digest preparing means 15 to the digital signature preparing means 19 via the time stamp means 21, The time acquired from the time acquiring means 23 later mentioned to data including the integrated digest received from said integrated digest preparing means 15 via this means of transmittal 17 is combined, A time stamp means 21 for it to be created by the digital signature preparing means 19 which creates a digital signature to this

united whole, and these each means, and to send the time stamp certificate containing the integrated digest, the time, and the digital signature which were acquired to the receiving means 25, It is constituted by the time acquiring means 23 which provides the time at the time of there being an inquiry by this time stamp means 21 as time information, and the receiving means 25 which receives the time stamp certificate sent from said time stamp means 21.

[0026]Here, the digest preparing means 11, the digest coupling means 13, the integrated digest preparing means 15, the means of transmittal 17, and the receiving means 25 constitute the client part 100, and the digital signature preparing means 19, the time stamp means 21, and the time acquiring means 23 constitute the server part 200.

[0027]Hereafter, with reference to drawing 1, the time stamp processing in a first embodiment is explained.

[0028]The object digital document G which consists of the text information created by the author, picture information, speech information, binary information, or those combination. By the digest preparing means 11 in the folder type time stamp system 1, while timing improvement in the speed of processing, It is made not to send the original document to the server part 200, and in order to obtain a value which is different with very high probability to a document different moreover, a hash function (for example, SHA-1 and MD5) is used for every digital document, and a digest is created.

[0029]If a hash function is specifically made into h, two or more digital document g_1 which constitutes the object digital document G, g_2, --, g_n, the digests h (g_1) and h (g_2), --, h (g_n) will be created by the digest preparing means 11.

[0030]Next, they are [each digests h (g_1) and h (g_2), --,] h (g_1) and h as a result of having combined h (g_n) by connection, by the digest coupling means 13, for example. -- (g_2) h (g_n) is obtained. An integrated digest is created by the integrated digest preparing means 15 from this joint result.

[0031]If the hash function used by the integrated digest preparing means 15 here is set to i, i (h (g_1), h (g_2) -- h (g_n)) will become an integrated digest. The integrated digest i (h (g_1), h (g_2) -- h (g_n)) is sent to the digital signature preparing means 19 via the time stamp means 21 by the means of transmittal 17.

[0032]The digital signature preparing means 19 creates digital signature s to the integrated digest i (h (g_1), h (g_2) -- h (g_n)) and the digital data containing the time t acquired by the time acquiring means 23, and sends out this digital signature s to the time stamp means 21.

[0033]Then, in the time stamp means 21, the time stamp certificate containing this digital signature s, and the integrated digest i (h (g_1), h (g_2) -- h (g_n)) and the time t is published, and it sends out to the receiving means 25.
[0034]By getting the independent organization which can set reliance periodically to the digital document on a personal computer to publish the time stamp certificate for existence proof according to a first embodiment, Also in the digital document which a related document, a figure, a table, etc. are united and constitutes one systematic document in many cases, The digital document on a personal computer is related with other digital documents on the personal computer which is creating those related document or them, and it becomes possible to acquire a time stamp certificate.
[0035]The reliability of the existence proof of the document which performed the time stamp can be improved, the digital document on a personal computer can be further considered as the same record as a research note or a housekeeping book in which a history remains daily, and it can utilize as a recording medium which can moreover prove the change creation record for a third party.
[0036]After the time of a time seal being pushed, two or more digital documents are not changed by this, and when surely a time seal is pushed, it becomes possible to prove that the digital document of these plurality existed simultaneously. And it is not necessary to judge the necessity of a time stamp certificate for every digital document, and in order for what is necessary to be collecting to two or more digital documents, and just coming to acquire one time stamp certificate, it becomes possible to utilize time stamp service by low cost.
[0037]Next, the composition of the folder type time stamp system concerning a second embodiment of this invention is shown in drawing 2.
[0038]In drawing 2, the folder type time stamp system 3, The digest preparing means 31 in which a text document, picture information, and speech information create the digest of the target object digital document G among the digital documents F contained suitably, The digest coupling means 33 which combines two or more digests created by this digest preparing means 31, The integrated digest preparing means 35 which creates an integrated digest to the result of the whole produced by combining two or more digests by this digest coupling means 33, The means of transmittal 37 which sends data including the integrated digest created by this integrated digest preparing means 35 to the digital signature preparing means 39 via the time stamp means 41, It combines with data including the integrated digest which received the time acquired from the time acquiring means 43a mentioned later from the integrated digest preparing means 35 via said means of transmittal 37, A time stamp means 41

for it to be created by the digital signature preparing means 39 which creates a digital signature to this united whole, and these each means, and to send the time stamp certificate containing the integrated digest, the time, and the digital signature which were acquired to the receiving means 45, The time acquiring means 43a which provides the time at the time of there being an inquiry by this time stamp means 41 as time information, The receiving means 45 which receives the time stamp certificate sent from said time stamp means 41, The verifying means 47 which verifies the time stamp certificate received via this receiving means 45, A time designated means 49 to direct the creation timing of a digest to said digest preparing means 31, The digital document setting means 51 which specifies the digital document made into an object from the digital document F, it is constituted by the time acquiring means 43b which provides said digest preparing means 31, the means of transmittal 37, the receiving means 45, and the time at the time of it having been alike, and receiving and there being an inquiry to the verifying means 47 as time information. The time acquiring means 43a and the time acquiring means 43b may be the same.

[0039]Here The digest preparing means 31 and the digest coupling means 33, The integrated digest preparing means 35, the means of transmittal 37, and the receiving means 45, The verifying means 47, the time designated means 49, the digital document setting means 51, and the time acquiring means 43b constitute the client part 100, and the digital signature preparing means 39, the time stamp means 41, and the time acquiring means 43a constitute the server part 200.

[0040]Hereafter, with reference to drawing 2, the time stamp processing in a second embodiment is explained.

[0041]As opposed to the digital document F which consists of the text on [from a personal computer] the accessible inside of a personal computer, or a network, a sound, a picture, binary information, or those combination, The object digital document G specified per the file or folder by the digital document setting means 51 is specified.

[0042]If it detects that the time specified by the time designated means 49 based on the time which the digest preparing means 31 acquired from the time acquiring means 43b came, the digest preparing means 31 receives the object digital document G, A digest is created using hash functions, such as SHA-1 and MD5, for every digital document.

[0043]In a hash function, if h and an object digital document are made into g_1, g_2---, and g_n, the digests h (g_1) and h (g_2), ---, h (g_n) will be created by the digest preparing means 31.

[0044]By the digest coupling means 33, as a result of combining h (g_n) by connection,

they are [the digests h (g_1) and h (g_2), --,] h (g_1) and h (g_2), for example. -- h (g_n) is obtained. An integrated digest is created by the integrated digest preparing means 35 from a joint result.

[0045]If the hash function used by the integrated digest preparing means 35 is set to i, i (h (g_1), h (g_2) -- h (g_n)) will become an integrated digest. The integrated digest i (h (g_1), h (g_2) -- h (g_n)) is sent to the digital signature preparing means 39 via the time stamp means 41 by the means of transmittal 37.

[0046]As opposed to the digital data containing the time t which acquired the digital signature preparing means 39 by the integrated digest i (h (g_1), h (g_2) -- h (g_n)) and the time acquiring means 43a, Digital signature s is created and this digital signature s is sent out to the time stamp means 41.

[0047]The time stamp means 41 publishes the time stamp certificate containing the integrated digest i (h (g_1), h (g_2) -- h (g_n)), the time t, and digital signature s, and sends it out to the receiving means 45.

[0048]The verifying means 47 verifies that it is the right digital signature by which the digital signature currently attached to the time stamp certificate received by the receiving means 45 was created by the digital signature preparing means 39.

[0049]It verifies that the time attached to the time stamp certificate is after the time which the means of transmittal 37 sent to the digital signature preparing means 39, and it is before the time which the receiving means 45 received.

[0050]As mentioned above, according to a second embodiment, it adds to the effect in a first embodiment, A time stamp certificate is periodically acquired to the file on the personal computer furthermore specified by the folder or the file basis, The series of the time stamp certificate which could record the creation change history of the file on a personal computer including the relation with a related file, and was acquired over long time can be used as the certificate by the third party to the creation change history of the file on a personal computer. Offer of the time stamp means by which it is reliable to a digital document more than a research note or a housekeeping book since forgery is difficult of the series of this time stamp certificate is attained.

[0051]Such a program for folder type time stamp systems mentioned above can improve the distributivity of the folder type time stamp program by recording on a recording medium and being provided using this recording medium.

[0052]Next, the composition of the distributed time stamp system concerning a third embodiment of this invention is shown in drawing 3.

[0053]In drawing 3, the distributed time stamp system 101, Fixed time information t_{1i} of unit width which a constant interval is set and is at least 1 time or more and which

exists independently respectively n times, --, two or more time acquiring means 113a, 113b, ---, 113s which acquire t_{si}, It is provided every every [these time acquiring means 113a and 113b, ..., / one] 113 s, and time information t_{ij} is combined with the digital document M, Two or more coupling means 111a, 111b, ..., 111s which create digital document Mt_{ij} with a time seal independently respectively, These coupling means 111a and 111b, ..., two or more digital signature means 115a, 115b, ..., 115s to be formed one [at a time] every 111 s, and to create a digital signature independently respectively, The digital signature means 115a and 115b of this plurality, ..., two or more digital signatures independently created in 115 s are received, Choose the digital signature mutually created from the equal digital document Mt with a time seal out of the digital signature of these plurality every [each digital signature means 115a and 115b, ..., / one] 115 s, and the digital document Mt equal to those selected each other with a time seal is received, Created digital signatures are consisted of by the integrated-digital-signatures preparing means 117 which creates integrated-digital-signatures c, and the time stamp certificate preparing means 119 which draws up the time stamp certificate T containing the digital document Mt with these time seals, and integrated-digital-signatures c.

[0054]Hereafter, with reference to drawing 3, the distributed time stamp processing in a third embodiment is explained. Although explanation is advanced focusing on the system of the coupling means 111a here, also in other systems, it is the same.

[0055]In the coupling means 111a in [the digital document M which consists of the text document drawn up by the author, picture information, speech information, binary information, or those combination to] the distributed time stamp system 101, It is combined with the time acquired by the time acquiring means 113a, and the digital document Mt with a time seal is drawn up. The digital signature to this drawn-up digital document Mt with a time seal is created by the digital signature means 115a. Thus, the digital signature created by each digital signature means 115a, 115b, ..., 115s is brought together in the integrated-digital-signatures preparing means 117.

[0056]Furthermore, the integrated-digital-signatures preparing means 117 creates integrated digital signatures from the digital signature to the digital document Mt with those common time with a time seal, when the one digital document Mt with common time with a time seal can choose every digital signature means 115. Then, the time stamp certificate preparing means 119 draws up the digital document Mt with a time seal used for creating integrated digital signatures, and the time stamp certificate T including integrated digital signatures.

[0057]Hereafter, an example is given and explained about digital signature creation.

Here, RSA public key encryption is used as an example of public key encryption.
[0058]First, p and q are made into a sufficiently big prime number, and it sets with n=pq. And phi(n) = (p−1) (q−1)
The relatively prime integer e is defined suitably. That is, gcd(e) =(q (p−1)−1) 1, and n and e are used as a public key, and it is ed=1 mod phi (n) about d.
When you come out and you consider it as a certain integer, let p, q, and d be secret keys.
[0059]The digest obtained with the application of a hash function (for example, SHA−1 and MD5) by the digital document Mt with common time with a time seal is set to m.
[0060]It sets with $c=m^d \bmod n$. Let c be integrated digital signatures eventually created by the integrated−digital−signatures preparing means 117 at this time. When the total of the digital signature means 115 in drawing 3 is set to s, d is expressed by the sum of a number, and it is $d=d_1+d_2+$. −− It sets with d_s.
[0061]If $c_1=m^{d1} \bmod n$, −−, $c_s=m^{ds} \bmod n$, c_s will serve as c_1, −−, a digital signature created by the s digital signature means 115a, 115b, ..., 115s. The digital document containing (Mt, c) turns into the time stamp certificate T.
[0062]Next, the composition of the distributed time stamp system concerning a fourth embodiment of this invention is shown in drawing 4.
[0063]In drawing 4, the distributed time stamp system 103, The receiving means 130 which receives the digital document M by communication, and n times which a constant interval is set and is at least 1 time or more, Fixed time information t_{1i} of unit width which exists independently respectively, −−, two or more time acquiring means 133a, 133b, ..., 133s which acquire t_{si}, Time information t_{ij} is combined with these time acquiring means 133a and 133b, ..., the digital document M that one was provided at a time every 133 s, and was received by the receiving means 130, Two or more coupling means 131a, 131b, −−−, 131s which create digital document Mt_{ij} with a time seal independently respectively, These coupling means 131a and 131b, ..., two or more digital signature means 135a, 135b, ..., 135s to be formed one [at a time] every 131 s, and to create a digital signature independently respectively, The digital signature means 135a and 135b of these plurality, ..., two or more digital signatures independently created in 135 s are received, The digital signature mutually created from the equal digital document Mt with a time seal out of the digital signature of these plurality is chosen every [each digital signature means 135a and 135b, ..., / one] 135 s, As opposed to the digital document Mt equal to those selected each other with a time seal, The integrated−digital−signatures preparing means 137 which creates integrated−digital−signatures c from the created digital signature, The time

stamp certificate preparing means 139 which draws up the time stamp certificate T containing the digital document Mt with these time seals, and integrated-digital-signatures c, It is constituted by the means of transmittal 141 which returns the sender of a digital document the time stamp certificate T drawn up by this time stamp certificate preparing means 139 by communication.

[0064]Drawing 5 and drawing 6 show the relation of the acquisition-times information in third and fourth embodiments. Here, the relation of acquisition-times information is shown for the case where there are three digital signature means in the example. In drawing 5 and drawing 6, t_{11}, t_{21}, and t_{31} express the time which three time acquiring means acquired to the 1st time, respectively, and t_{12}, t_{22}, and t_{32} express the time which three time acquiring means acquired to the 2nd time, respectively. t_{i1}, t_{i2}, and t_{i3} express exact time when three time acquiring means perform time acquisition to the 1st time, respectively, t_{j1}, t_{j2}, and t_{j3} express exact time when three time acquiring means perform time acquisition to the 2nd time, respectively.

[0065]It means having acquired the time information same to the 1st time also as three time acquiring means, and having acquired as same the time information as the 2nd time in drawing 5. In this case, $t_{11}=t_{21}=t_{31}$ serves as time used for creation of integrated digital signatures. Similarly, it expresses having acquired the time information with the 1st same time of the third time acquiring means in drawing 6 as the 2nd time of the second time acquiring means for a start. In this case, $t_{31}=t_{12}=t_{22}$ serves as time used for creation of integrated digital signatures.

[0066]Drawing 7 shows the relation between the exact time at the time of the time acquisition at the time of cutting fine as compared with drawing 6, and making width into a half, and acquisition-times information. In drawing 7, t_{11}, t_{21}, and t_{31}, Express the time which three time acquiring means acquired to the 1st time, respectively, and t_{12}, t_{22}, and t_{32}, Expressing the time which three time acquiring means acquired to the 2nd time, respectively, t_{13}, t_{23}, and t_{33} express the time which three time acquiring means acquired to the 3rd time, respectively. t_{i1}, t_{i2}, and t_{i3} express exact time when three time acquiring means perform time acquisition to the 1st time, respectively, t_{j1}, t_{j2}, and t_{j3} express exact time when three time acquiring means perform time acquisition to the 2nd time, respectively, t_{k1}, t_{k2}, and t_{k3} express exact time when three time acquiring means perform time acquisition to the 3rd time, respectively. In the example which made this unit width the half, in order to acquire the same time information by three time acquiring means, each time acquiring means needs to perform at least three time acquisition.

[0067]Although the constant interval to which each time acquiring means performs

time acquisition can be set as arbitrary length, it is preferred to set up equally to the fixed unit width of the time which each time acquiring means acquires.

[0068]It is also possible to make into the acquisition times of the 2nd henceforth time produced at the time acquired to the 1st time by adding the time of the fixed unit width decided beforehand one by one, without performing time acquisition of the 2nd henceforth actually. In this case, each time acquiring means may only perform time acquisition once.

[0069]Although the fixed unit width of the time which each time acquiring means acquires can be set as arbitrary length, The more it makes unit width small, while the accuracy of the time acquired improves the more, the number of the digital signatures which each digital signature means will create will increase until the one digital document Mt with common time with a time seal can choose for every digital signature means.

[0070]However, when time for the digital document M to reach each coupling means has dispersion. It is possible to reduce the number of digital signatures, as creation of the digital signature to at least one of the time which is not used as common time by any means as follows in the digital signature means corresponding to coupling means other than the coupling means which starts most as for time is not performed.

[0071]Drawing 8 expresses the relation of time width which a digital document may reach to two different coupling means. (1) of drawing 8 expresses the case where a digital document cannot arrive at another coupling means only after the time which a digital document is the latest and may reach one coupling means, and (2) of drawing 8, The time when a digital document may reach one coupling means latest is contained in the time zone when a digital document may reach another coupling means, And express the case where the time when a digital document may reach the former coupling means early most becomes the latter coupling means before the time when a digital document may arrive early most, and (3) of drawing 8, The case where the time zone when a digital document may reach one coupling means is thoroughly contained in the time zone when a digital document may reach another coupling means is expressed. The relation of the time zone when the same digital document as two arbitrary coupling means arrives becomes these three either.

[0072]Drawing 9 expresses the context of a in case the time-of-arrival belt to the coupling means which a digital document reaches latest is during the time c and d and the time zone when a digital document reaches the other arbitrary coupling means is during the time a and b, b, c, and d. (1) of drawing 9, (2), and (3) show the case equivalent to (1) of drawing 8, (2), and (3), respectively. The coupling means which a

digital document reaches latest here is set to C1, and the other arbitrary coupling means are set to C2. The interval of unit width, i.e., t_i, and t_{i+1} is set to u.

[0073]Generally each coupling means makes start time time produced at the time of the latest after current time decided beforehand by adding zero or more time beforehand specified in order to remove the time which is not used on integrated-digital-signatures creation by any means here, It is possible to draw up a digital document with a time seal by combining with a digital document by making into time information time of the specification number obtained with the time interval specified beforehand.

[0074]Here, when the arrival time of a digital document has a fixed gap between coupling means, zero or more time specified beforehand is used in order that the coupling means which starts digital document preparation with a time seal previously may originally delay the start of digital document preparation with a time seal according to the gap.

[0075]Also when the time width of the arrival time of the digital document in a coupling means may have change, the specification number is used in order to call for the digital document with a time seal of the time which is common to every digital signature means so that integrated digital signatures can certainly be made.

[0076]Since current time is e and it is n= 1 supposing it sets to v a product with the greatest integral values n and u that do not exceed (c-b)/u in the case of (1) of drawing 9 and a digital document reaches C2 at the time e between time t_3 and t_4, It is possible for t_4 and zero or more time specified beforehand to set to v=n*u=1*u time when it was beforehand decided after current time. The time interval specified beforehand is u, and after the specification number adds 1 to the minimum integral value m more than (d-a)/u, it can be considered as the number of ** which lengthened n. In this case, since it is m= 5, the specification number is set to 5+1-1=5.

[0077]As a result, it is not necessary to draw up the digital document with a time seal which makes t_4 time information. What is necessary is to draw up only the digital document with a time seal which makes time information t_5 of the five specification number from t_5 produced by adding v to t_4, t_6, t_7, t_8, and t_9. What is necessary is to draw up only the digital document with a time seal which makes t_4, t_5, t_6, t_7, and t_8 time information similarly, when e is between a and t_3. What is necessary is to draw up only the digital document with a time seal which makes t_6, t_7, t_8, t_9, and t_{10} time information similarly, when e is between t_4 and b.

[0078]Supposing a digital document reaches C2 at the time e between time t_3 and t_4 in the case of (2) of drawing 9, current time is e and it is possible for t_4 and zero or more

time specified beforehand to set to 0 time when it was beforehand decided after current time. The time interval specified beforehand is u and the specification number can be considered as the number which added 1 to the minimum integral value m more than (d−a)/u. In this case, since the specification number is set to 6, only the digital document with a time seal which makes a hour entry t_4, t_5, t_6, t_7, t_8, and t_9 will be drawn up.

[0079]Supposing a digital document reaches C2 at the time e between time t_5 and t_6 in the case of (3) of drawing 9, current time is e and it is possible for t_6 and zero or more time specified beforehand to set to 0 time when it was beforehand decided after current time. The time interval specified beforehand is u and the specification number can be considered as the number which added 1 to the minimum integral value m more than (d−a)/u. In this case, since the specification number is set to 3, only the digital document with time which makes t_6, t_7, and t_8 a hour entry will be drawn up.

[0080]Now, if it is in a distributed time stamp system, usually, Since the digital signature means of a component distributes and holds some secret keys in public key encryption, Since a possibility that the time which the time acquiring means acquired independently respectively is in agreement is very small as what can be made small mentioned above the theft of a secret key, and the danger of forgery of a time stamp certificate, there is a problem that integrated digital signatures cannot be created.

[0081]On the other hand, in a third and fourth embodiment, since time is acquired by fixed unit width as mentioned above, a possibility that the time acquired independently respectively will become equal can be made high. In the example shown in drawing 5 and drawing 6, if a constant interval is set and at least two time acquisition is performed for every time acquiring means, it will actually become possible to obtain the digital document with a time seal which is certainly common by all the coupling means from unit width and the relation of the time acquisition execution time difference between time acquiring means. As a result, the distributed time signature which raises the safety of a secret key is attained.

[0082]Such a distributed time stamp program can improve the distributivity of the distributed time stamp program concerned by recording on a recording medium and being provided.

[0083]Although a third and fourth embodiment mentioned above explained the case where RSA was used for public key encryption, This invention divides secret keys, such as elliptic curve public key encryption and DSA (Digital Signature Algorithm), without being limited to this, Even if it uses the public key encryption which can create the same digital signature as the digital signature created with a single secret

key from two or more divided secret keys, it is possible to create a digital signature and integrated digital signatures similarly.

[0084]Even if it creates integrated digital signatures using the digital document which contains the digital document Mt with a time seal instead of the digital document Mt with a time seal, it is satisfactory in any way. It is also possible to create a digital signature directly, without furthermore applying a hash function to a digital document. One time information may be made to correspond to the one digital document Mt with a time seal, and two or more time information may be made to correspond to the one digital document Mt with a time seal. That is, when it corresponds to one time information, one digital signature is created from the one digital document Mt with a time seal, and when it corresponds to two or more time information, two or more digital signatures will be created from the one digital document Mt with a time seal.

[0085]Next, the composition of the folder type distribution time stamp system concerning a fifth embodiment of this invention is shown in drawing 10. This fifth embodiment combines the first and a second embodiment which were mentioned above, and third and fourth embodiments.

[0086]In drawing 10, the folder type distribution time stamp system 300 consists of the client part 100 and the server part 200. The client part 100 creates the time stamp demand R from two or more digital documents G which are time stamp objects, and passes it to the server part 200. The server part 200 draws up the time stamp certificate T based on the received time stamp demand R, and returns it to the client part 100.

[0087]The example of 1 composition of the client part 100 in the folder type distribution time stamp system 300 of drawing 10 is shown in drawing 11. The client part 100 of drawing 11 is equivalent to the client part 100 of drawing 2 in a second embodiment mentioned above, and has given identical codes to the identical configuration element.

[0088]First, the digital document G which is the target of a time stamp out of the set F of a digital document is chosen by the digital document setting means 51.

[0089]Next, in the periodical digest creation time specified by the time designated means 49, a digest is created for every digital document with the selected digest preparing means 31. After creating a digest last time here, about the digital document which does not have change in the contents, it is also possible to use the digest created last time.

[0090]Next, by the digest coupling means 33, the digest which the digest preparing means 31 created about each of the object digital document G is combined, and one

new digital document is drawn up.
[0091]Next, an integrated digest is created from this new digital document by the integrated digest preparing means 36.
[0092]And the time stamp demand R including an integrated digest is sent to the server part 200 from the means of transmittal 37.
[0093]In the server part 200, the time stamp certificate T is drawn up so that it may mention later, and it sends to the receiving means 45 of the client part 100.
[0094]Next, sending time according [the verifying means 47] to the means of transmittal 37 and receipt time by the receiving means 45, That the digital signature which compares the attestation time currently recorded on the received time stamp certificate T, and also is contained in the time stamp certificate T is a genuine digital signature created by the server part 200, It verifies using the public key corresponding to the secret key which the server part 200 used, and also it is verified whether the digest by which the time stamp is carried out with the time stamp certificate T is sent by the means of transmittal 37.
[0095]It becomes possible by including the last time stamp certificate in the object digital document G here to acquire a time stamp certificate including creation of the past of the object digital document G, and a change history.
[0096]The example of 1 composition of the server part 200 in the folder type distribution time stamp system 300 of drawing 10 is shown in drawing 12. The server part 200 of drawing 12 is equivalent to the distributed time stamp system of drawing 4 in a fourth embodiment mentioned above, and has given identical codes to the identical configuration element.
[0097]First, if the receiving means 130 receives the time stamp demand R, the copy will be sent to each coupling means 131.
[0098]Next, each coupling means 131 combines the digital document M contained in the time acquired by the applicable time acquiring means 133 and the time stamp demand R, and draws up the digital document Mt with a time seal.
[0099]Next, it creates with the partial secret key which acquires beforehand the digital signature to this drawn-up digital document Mt with a time seal in a digital signature means 135 to correspond. Thus, the digital signature created by each digital signature means 135 is brought together in the integrated-digital-signatures preparing means 137.
[0100]Next, out of the collected digital signature, the integrated-digital-signatures preparing means 137 chooses one digital signature with common time information per digital signature means 135, and creates integrated digital signatures.

[0101]And the time stamp certificate preparing means 139 draws up the time stamp certificate T using the created integrated digital signatures, and this is sent to the client part 100 from the means of transmittal 141.

[0102]Other examples of composition of the server part 200 in the folder type distribution time stamp system 300 of drawing 10 are shown in drawing 13. Drawing 13 shows the distribution composition which employs the function of the server part 200 by the independent independent organization, and has given identical codes to the server part 200 and identical configuration element of drawing 12 which were mentioned above.

[0103]in drawing 13 -- the coupling means 131, the time acquiring means 133, and the digital signature means 135 -- every one lot each the one distributed partial time stamp organization 205, [constitute and] Although it differs from drawing 12 in that the receiving means 130, the integrated-digital-signatures preparing means 137, the time stamp certificate preparing means 139, and the means of transmittal 141 constitute the one time stamp organization 204, operation of each means is the same as the case of drawing 12.

[0104]

[Effect of the Invention]It is considered as the record in which a history remains daily by acquiring the time stamp certificate for existence proof from the independent organization which can set reliance periodically to the digital document on a personal computer according to the folder type time stamp system of this invention as mentioned above, And it becomes possible to prove change creation record for a third party.

[0105]Since it becomes possible to obtain the digital document with a time seal which is certainly common by all the coupling means according to the distributed time stamp system of this invention, the distributed time signature which raises the safety of a secret key is attained.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]The block diagram showing the example of composition of the folder type time stamp system in a first embodiment of this invention.

[Drawing 2]The block diagram showing the example of composition of the folder type time stamp system in a second embodiment of this invention.

[Drawing 3]The block diagram showing the example of composition of the distributed time stamp system in a third embodiment of this invention.

[Drawing 4]The block diagram showing the example of composition of the distributed time stamp system in a fourth embodiment of this invention.

[Drawing 5]The figure showing an example of the acquisition-times information acquired in drawing 3 and the distributed time stamp system of drawing 4.

[Drawing 6]The figure showing other examples of the acquisition-times information acquired in drawing 3 and the distributed time stamp system of drawing 4.

[Drawing 7]The figure showing other examples of the acquisition-times information acquired in drawing 3 and the distributed time stamp system of drawing 4.

[Drawing 8]The figure showing the relation of the time width to which a digital document may reach two different coupling means in drawing 3 and the distributed time stamp system of drawing 4.

[Drawing 9]The figure showing the example of the time width and the arrival time when a digital document may reach two different coupling means in drawing 3 and the distributed time stamp system of drawing 4.

[Drawing 10]The block diagram showing the example of composition of the folder type distribution time stamp system in a fifth embodiment of this invention.

[Drawing 11]The block diagram showing the example of 1 composition of the client part in the folder type distribution time stamp system of drawing 10.

[Drawing 12]The block diagram showing the example of 1 composition of the server part in the folder type distribution time stamp system of drawing 10.

[Drawing 13]The block diagram showing other examples of composition of the server part in the folder type distribution time stamp system of drawing 10.

[Description of Notations]

1 and 3 Folder type time stamp system

11, 31 digest preparing means

13 and 33 Digest coupling means

15 and 35 Integrated digest preparing means

17 and 37 Means of transmittal

19, 39 digital-signature preparing means

21 and 41 Time stamp means
23 and 43 Time acquiring means
25 and 45 Receiving means
47 Verifying means
49 Time designated means
51 Digital document setting means
100 Client part
101,103 Distributed time stamp system
111,131 Coupling means
113,133 Time acquiring means
115,135 digital signature means
117,137 integrated-digital-signatures preparing means
119,139 Time stamp certificate preparing means
130 Receiving means
141 Means of transmittal
200 Server part
300 Folder type distribution time stamp system
M Digital document
T Time stamp certificate
R Time stamp demand

[Translation done.]